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[†]

Work Package 4: Policy and the European dimension

Deliverable D4.2: 2nd year report on Cybersecurity Threats

Abstract: Based on the 1st year report on cybersecurity threats, the present document provides an advanced overview of the cybersecurity threat landscape from a technological, legal/policy and economic perspective. The discussion surfaces existing gaps and challenges, points at the practices associated with the implementation of cybersecurity at an organizational level and provides for early-stage recommendations to be refined under the 3rd year report on cybersecurity threats. Capturing the momentum, specific focus is given to the impact of COVID-19 pandemic on the threats' landscape per se, on the insights gained and, on the actions, so far taken. This Deliverable D4.2 constitutes the outcome of specific activities, which took place in 2020, such as desk research and qualitative research. The latter was mainly in the form of interviews with project partners involved in (a) the sectorial CONCORDIA pilots, (b) CONCORDIA's threat intelligence sharing pilot and (c) cybersecurity certification.

Contractual date of delivery	*M24*
Actual date of delivery	*30.12.2020*
Deliverable dissemination level	*Public*
Editors	*Arthur van der Wees, Dimitra Stefanatou, Prakriti Pathania (ALBV)*

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

Contributors	*Claudio Ardagna, Marco Anisetti, Nicola Bena, Ernesto Damiani (UMIL),* *Arthur van der Wees, Dimitra Stefanatou, Prakriti Pathania (ALBV),* *Tatjana Welzer Družovec, Urška Kežmah (UM),* *Drivas, George, Maglaras, Leandros (GSDP),* *Muriel Franco, Burkhard Stiller (UZH)*
Quality assurance	*TÜV TRUST IT GmbH, EFACEC, CODE, FORTH*

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
SURFnet bv	SURFnet 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~~
GSDP	Ministry of Digital Policy, Telecommunications and	Greece

	Media	
RISE	RISE Research Institutes of Sweden AB	Sweden
Ericsson	Ericsson AB	Sweden
SBA	SBA Research gemeinnutzige 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	EOTVOS LORAND TUDOMANYEGYETEM	Hungary
Utimaco	Utimaco Management GmbH	Germany

Document Revisions & Quality Assurance

Internal Reviewers

1. EFACEC (review lead)
2. TUV Austria
3. CODE
4. FORTH

Revisions

Ver.	Date	By	Overview
0.01	15.09.2020	ALBV	*Deliverable Structure and Methodology*
0.02	09.10.2020	UMIL	*Technological Perspective (initial input))*
0.03	13.10.2020	UZ	*Economic Perspective*
0.04	19.10.2020	ALBV	*Introduction*
0.05	25.10.2020	ALBV, UM	*Legal Perspective (initial input)*
0.06	13.11.2020	ALBV	*Updates on the Legal Perspective*
0.07	27.11.2020	UMIL	*Technological Perspective (final input))*
0.08	29.11.2020	ALBV	*Executive Summary, Conclusions, Legal Perspective (final input)*
1	30.11.2020	ALBV	*Final version for internal review ready (1 round).*
1.01	10/12/2020	Forth, TUV, EFACEC	*1st version after revision*
1.02	15.12.2020	UZH	*Integration of revised input under the Economic Perspective.*
1.03	16.12.2020	UMIL, ALBV	*Integration of revised input under the Technological Perspective and the Legal Perspective*
2	17.12.2020	ALBV	*Final version for internal review ready (2nd round).*

Executive Summary

2020 has been a watershed year for the global economy as it underwent seismic changes on almost every front by virtue of the COVID-19 pandemic. The accelerated and large adoption of digital technologies during the pandemic and the subsequent surge in cyber-attacks and cybercrime underscores the relevance of CONCORDIA project as a whole and of this deliverable in particular. Moreover, it reiterates the fact that cybersecurity is not a "nice-to-have" but a "need-to-have."

D4.2 is the second of three consecutive deliverables under WP4 on Policy and the European dimension that includes D4.1: 1st Year Report on Cybersecurity Threats and D4.3: 3rd Year Report on Cybersecurity Threats. These three deliverables provide a broad overview of the ever evolving and dynamic cybersecurity landscape from different perspectives, namely, the technological perspective, the legal/policy perspective and the economic perspective. To maintain consistency with its predecessor deliverable D4.1, the present deliverable navigates through the evolving cybersecurity landscape in the same three-tiered manner, as summarised below.

Following the presentation of the latest policy developments pertinent to the scope of the present document both at European and International level *(Chapter 1)* and the illustration of the CONCORDIA environment *(Chapter 2), Chapter 3* elaborates on the *Technological Perspective.* In this context, the Chapter 3 first builds on the emerging threats and evolving attacks discussed in D4.1 and adds new cybersecurity threats, including those presented during the COVID-19 pandemic. More specifically, the discussion produces an assessment of the impact of COVID-19 on the cybersecurity threat landscape and on its impact on the cybersecurity gaps and challenges in the six (6) domains of interest for CONCORDIA, namely, network-centric, system-centric, application-centric, data-centric, user-centric, and IoT/Device-centric security. *Chapter 3* later provides for the key takeaways so far identified.

The *Legal Perspective (Chapter 4)* provides an update on the regulatory framework put forth in D4.1. which includes the existing legislations relevant to this deliverable as well as legislations that are still in the pipeline. This section highlights the relevance of certain legislations such as the NIS Directive, the GDPR and the Cybersecurity Act in the context of the COVID-19 pandemic. It, also, touches upon the recently proposed Data Governance Act [1], putting forward a "data-centric" approach. Based on information from several interviews, conducted during 2020 with project partners involved in the sectorial CONCORDIA pilots, in CONCORDIA's threat intelligence sharing pilot and in cybersecurity certification activities. The section elaborates on the challenges linked to cybersecurity at the level of implementation.

Finally, following the exploration of the "state of play" of cybersecurity through regulations and practices, the section produces early recommendations to be refined in Year 3.

Note, that at the time of finalising this deliverable (first half of December 2020), the European Commission published a series of policy making documents and legislative proposals, including the new EU Cybersecurity Strategy, the revised Directive on Security

[1] 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

of Network and Information Systems (NIS 2 Directive), the proposal for the Digital Services Act and the proposal for Digital Market Act. Due to the overlap in timing, these updates have not been captured in the present deliverable. However, the impact of these recent developments on the cybersecurity landscape will be taken into account in the subsequent deliverable i.e., D4.3: 3rd Year Report on Cybersecurity Threats.

Furthermore, the *Economic Perspective (Chapter 5)* presents new approaches for risk assessment, planning, and investments in cybersecurity wherein it discusses a) SERViz, a visual tool for analysing risks and planning investments in cybersecurity b) MENTOR, a recommendation system to help determine a solution that would provide an appropriate protection level based on specific business requirements and c) SecBot, a conversational agent for cybersecurity planning and management. Each approach includes case studies that were conducted to reflect their feasibility.

Overall, in Year 2, activities in T4.1, T4.2, T4.3 have been proceeding, as planned. COVID-19 pandemic has been taken into account under the respective activities and, therefore, the present deliverable encapsulates the respective output (e.g. the impact of COVID-19 on the evolving cybersecurity threat landscape. From an operational point of view, the COVID-19 pandemic, however, neither affected the performance of the research activities and of other type of work, that preceded the drafting of the present deliverable nor the drafting itself of this deliverable.

Contents

1. Introduction

Digital technologies are constantly transforming people's lives, revolutionising the world of work and reinventing society. They have enabled organisations to strategically improve services, expand into different markets, develop innovative products and services and gain competitive advantage on an international level. For the public sector, they have drastically improved access to public services, facilitated stronger citizen engagement and provided a wide variety of additional benefits including more efficiency and savings for both governments and businesses.[2]

For the last few years, digital technologies have been high on the agenda of the European Commission as well. By driving new initiatives, strategies, policies and legislation with a clear focus on data, technology, and infrastructure, the Commission is set to make this Europe's "Digital Decade." Moreover, the Digital Economic and Society Index (DESI) 2020 has revealed that Member States have bolstered their digital performance over the past year.[3] The DESI report also underscores the crucial role that digital technologies have played during the ongoing COVID-19 pandemic by enabling people to continue working, tracking the spread of the virus, and expediting the search for a cure.

However, with an increasing adoption of digital technologies in the EU, the topic of cybersecurity has gained significant traction. A recent study that interviewed approximately 27,607 EU citizens from different Member States revealed that 76% of the participants were of the view that there was an increasing risk of them being a victim of cybercrime.[4] Additionally, 46% of the participants were concerned about misuse of their personal data while 41% were concerned about the security of online payments. On similar lines, the Tallinn Manual[5] which deals with applicability of international law to cyber operations was revamped in 2016 to explore how the cyber threat landscape has evolved since the release of its initial version in 2013. From conventional state-authorized and operated cyber warfare, the revamped version of the Manual shifts focuses on common cyber incidents that are encountered by states on a more regular basis in today's time.

As it will be demonstrated in the discussion below, while the COVID-19 pandemic has pushed the global economy into "unchartered territory" with countries scrambling to control the virus, it has also served as an eye-opener regarding existing inefficiencies and unpreparedness for the unexpected. Organisations, governments and societies across the globe are now moving towards re-designing and aligning to the "new normal", pivoting their processes and strategically collaborating with organisations to ensure business continuity as well safety of individuals.

Keeping the above developments in mind and building on the areas highlighted in D4.1, this section presents the policy context and relevant updates that have taken place since the publishing of the first deliverable i.e., D4.1[6] of the three consecutive deliverables (D4.2 and

[2] Digital Economy and Society Index (DESI) 2020, Digital public services, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=67084
[3] Digital Economy and Society Index (DESI) 2020, Thematic chapters, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=67086
[4] Special Eurobarometer 499, Europeans' attitudes towards cyber security, available at: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/89090
[5] Schmitt, M. (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (2nd ed.). Cambridge: Cambridge University Press
[6] CONCORDIA Deliverable D4.1: 1st year report on cybersecurity threats

D4.3 to follow). It subsequently provides an overview of the methodology used and the structure of the document and in WP4 in general.

1.1. The Policy Context

The ongoing pandemic drastically increased dependence on technology across all industries and also put cybersecurity capabilities of organisations to the test. As per a report by the European Union Agency for Cybersecurity (ENISA), cyberattacks are becoming more sophisticated, targeted and are going undetected.[7] The most critical threats include data theft, financial fraud, personal information theft, email phishing and attacks against heath organisations. Overall, as argued by the Commissioner of Internal Market, Thierry Breton, the impact of COVID-19 pandemic has been so significant that "in the first 100 days of managing the COVID pandemic, more European credos have tumbled than in 30 years", surfacing among other -also- the necessity for the establishment of Digital Sovereignty.[8]

More specifically, in response to COVID-19, the EU has mobilised all resources to enable Member States to coordinate their national response. The Digital Strategy adopted by the European Commission in February 2020 gained renewed importance as the Commission and other organisations leverage digital technologies to monitor the spread of the COVID-19 virus.[9] The European Digital Strategy focuses on, among others, the need to build a strong EU legal framework relating to data protection, fundamental rights, safety and cybersecurity. Further, the Recovery Plan for Europe will be channelling recovery investment towards strategic digital capacities and capabilities including cybersecurity.[10]

In this respect, the EU Security Union Strategy for 2020 to 2025 is another initiative wherein the European Commission acknowledges that new technologies enabled organisations to function despite the pandemic.[11] However, it reiterates along with its benefits, the use of such technologies also brings concomitant risks and uncertainties. The Strategy calls for a "whole-of-society approach" which involves EU institutions, agencies, Member States, academia, industry and individuals in order to give cybersecurity the priority that it needs. The European Commission has also identified the need for establishing a Joint Cyber Unit (JCU) so as to ensure structured and coordinated operational cooperation. The JCU will foster trust between the different actors and stakeholders within the cybersecurity ecosystem and provide a key service to Member States.

From a legislative perspective, the NIS Directive which was adopted in July 2016 to bolster overall level of cybersecurity in the EU is currently being reviewed by the Commission.[12]

[7] ENISA Main Incidents in the EU and Worldwide, available at: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl-2020-main-incidents

[8] More information can be found at: https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-end-naivety_en

[9] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

[10] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, , Europe's moment: Repair and Prepare for the Next Generation, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1590732521013&uri=COM%3A2020%3A456%3AFIN

[11] Communication from the Commission on the EU Security Union Strategy, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX:52020DC0605

[12] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union OJ L 194

While Article 23 of the NIS Directive provides for periodical reviews of the functioning of the Directive, this initiative is also in line with the Commission's key policy to make "Europe fit for the Digital Age." For this purpose, a consultation was launched in July 2020, the results of which will be used for the evaluation and review which is expected to take place by the end of 2020. Pursuant to the EU Cybersecurity Act, the Commission is also working on an EU-wide certification framework for ICT digital products, services and processes.[13] The certification framework will facilitate EU-wide certification schemes that aim at providing criteria to carry out conformity assessments so as to create a standard level of adherence for products, services and processes against specific requirements. In July 2020, ENISA launched a public consultation to enable stakeholders and interest parties to provide their feedback on the first candidate cybersecurity certification scheme, the Common Criteria based European cybersecurity certification scheme (EUCC).

Interestingly, the Council of the EU imposed first ever sanctions in July 2020 against six individuals and three organisations for their involvement in certain cyber-attacks.[14] The sanctions were in response to cyberattacks that had a significant impact including the cyber-attacks publicly known as 'WannaCry' and 'NotPetya', that resulted in significant damage and economic loss to the EU as well as the attempted cyber-attack against the Organisation for the Prohibition of Chemical Weapons (OPCW) in the Netherlands. The sanctions set out in the Annex to Decision (CFSP) 2019/797 included travel bans as well as an asset freeze. Moreover, EU persons and organisations have been forbidden from providing funds or economic resources to the listed individuals and organisations. [15]

For the last few years, the EU has consistently taken steps forward as far as cybersecurity is concerned. Initiatives at an EU as well as Member State level have facilitated a strategic and harmonised approach to bolster processes and capabilities in the wake of increasing cybersecurity threats and data breaches. The COVID-19 pandemic presented opportunities for government agencies and other organisations to rethink and redesign existing process and strategies. Note, that -even at the time of finalising this deliverable(first half of December 2020)- the European Commission published a series of policy making documents and legislative proposals, including the new EU Cybersecurity Strategy[16], the revised Directive on Security of Network and Information Systems (NIS 2 Directive)[17], the proposal for the Digital Services Act[18] and the proposal for the Digital Market Act.[19] Due to the

[13] 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) OJ L 151

[14] Council Decision (CFSP) 2020/1127 f 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32020D1127&from=EN

[15] Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019D0797

[16] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

[17] 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, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166

[18] 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://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN

[19] 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://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN

overlap in timing, these updates have not been captured in the present deliverable. However, the impact of these recent developments on the cybersecurity landscape will be taken into account in the subsequent deliverable i.e., D4.3: 3rd Year Report on Cybersecurity Threats.

1.2. Methodology[20]

Building on D4.1, Deliverable D4.2 is the second of three consecutive deliverables (D4.2 and D4.3 to follow) focusing on cybersecurity threat analysis. These three deliverables will outline (a) the landscape of current and emerging threats and evolving attacks, by providing an end-to-end overview of cybersecurity threats, including current security gaps and challenges, existing countermeasures and future research actions (technological perspective in Task T4.1), (b) the landscape of the most relevant currently applicable and other possibly forthcoming in EU, addressing -also- state of play of cybersecurity at the level of implementation and proposing how to improve it towards the state of the art EU (legal perspective in Task T4.2), and (c) the economic aspects of cybersecurity, especially from an economic analysis approach (economics perspective in Task T4.3). Note that the six (6) domains of interest, namely, network-centric, system-centric, application-centric, data-centric, user-centric, IoT/device-centric security underlying the approach taken under D4.1 remain relevant.

Technological perspective

Task T4.1 aims to produce threat reports focusing on the domains of interest of CONCORDIA (Section 2.1), as well as establishing liaisons and collaborating closely with the relevant European experts and stakeholders and contributing to the cybersecurity roadmap for Europe in Task T4.4.[21]

Activities in T4.1 are composed of three main phases. The first phase (emerging threats and evolving attacks) have been 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 domains of interest of CONCORDIA (Section 2.1). This phase reported in D4.1 collected relevant documents from literature, including white papers and reports (e.g., ENISA threat landscape, 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. This phase provided an overview of assets, threats, and attacks, shaping the current trends in cybersecurity. The second phase (gaps and challenges) is reported in this deliverable. It analyses and discusses gaps and challenges with respect to identified threats and vulnerabilities and manages crosscutting aspects of the threat landscape affecting more domains of interest. The third step (countermeasures) will provide a set of guidelines and an overview of existing countermeasures. A list of research actions will be also provided to shape the future research to the aim of mitigating identified threats and risks.

Activities in T4.1 have been/ will be fed in three different deliverables that provide an overview of technological findings as follows.

[20] For consistency and readability purposes, this section is -to an extent-based on the related section under D4.1: 1st Year *report on cybersecurity threats,* capturing further updates pertinent to the scope of the present document.

[21] A first version of this cybersecurity threat analysis has been presented at CONCORDIA Open Door held in Luxembourg, October 2019

- D4.1 presented a first threat analysis and state-of-the-art overview.
- D4.2 (this deliverable) refines the threat analysis and focuses on crosscutting aspects of threat analysis, as well as gaps and challenges.
- D4.3 will provide the final threat analysis and discussion on future research actions and countermeasures.

Activities in T4.1 build on the competences of partners in CONCORDIA, benefiting from their direct contributions. To this aim, we started different working groups in the domains of (i) Device/IoT-centric, (ii) network-centric, (iii) system-centric, (iv) datacentric, (v) application-centric, and (vi) user-centric security. Each of the working groups produced a section of this deliverable (Section 3.3-Section 3.8), elaborating on gaps and challenges in the area that is addressed by each working group.

Legal perspective

In the spirit of a human-centric approach to cybersecurity, the legal perspective puts particular emphasis on the organizational measures employed by organisations of all sizes participating in the project in view of ensuring compliance with the requirements set under EU law. Taking into account the regulatory landscape illustrated under D4.1 and the reality of cybersecurity at an implementational level, the legal perspective aims at producing a set of recommendations aiming to strengthen the effectiveness of existing rules and creating an organizational culture around cybersecurity.

Notably, based on the planning concerning the legal perspective as elaborated under D4.1, T4.2 aimed at focusing on the "state of play" in relation to the most relevant regulations pertinent to cybersecurity and organizational practices (Year 1 and Year 2), in order to produce recommendations on how to reach the "state of the art" at a later project stage (Year 3). Nevertheless, T4.2 delivers -upon reviewers' request- a set of early recommendations in advance (Year 2)[22].

The work of T4.2 comprises of both desk research, as well as qualitative research in the form of interviews with consortium partners to be elaborated further in the discussion to follow. In particular, these interviews were conducted -in this year 2, initially - with representatives of the sector-specific CONCORDIA pilots as well as from CONCORDIA's threat intelligence respectively certain certification perspectives. In the context of these interviews, COVID-19 pandemic has been -also- to an extent addressed.

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

- D4.1 illustrated the regulatory environment by providing an overview of the most relevant current and proposed European regulations.
- D4.2 (this deliverable) produces an update of the regulatory developments and further addresses the actual practices aiming to safeguard cybersecurity at an organizational level, based, also, on input collected directly from CONCORDIA partners -primarily- from the sector specific pilots, namely, from the pilots in the

[22] Following reviewers' comments, T4.2 has adjusted its' planning accordingly and - to the extent possible, given the submission date of D4.2 (December 2020) and the time of the receipt of reviewers' comments (October 2020), provides for early recommendations under the present document.

aerospace sector, the e-health sector, the threat intelligence sector and the financial sector. [23] Moreover, it provides for a set of early recommendations, to be further matured in Year 3.
- D4.3 will put forward the final recommendations on how to create an organizational culture on cybersecurity.

Economics perspective

The economics perspective maps actors, responsibilities, inter-dependencies, and risks involved and relevant for cybersecurity, to provide a basis for economic analysis models, ready to analyse and determine measurable factors in the area of cybersecurity mechanisms. These models can provide an accurate picture of cybersecurity economic impacts, thus helping stakeholders during the analysis of economic impacts of threats and 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 cyber-attacks (e.g., governments, companies, and the financial sector). Thus, in the light of such information, a novel framework is proposed for estimating costs in complex distributed systems, which provide models for cost estimations and mapping of relations between interdependent systems and their components.

Activities conducted within the T4.3 will provide outcomes for different deliverables and activities within the CONCORDIA, which include:
- D4.1 provided a discussion about the economic impacts of cybersecurity and introduces a phase-based framework called SEConomy for the risk assessment and analysis of cybersecurity investments. Also, based on highly specific threats and risks analysed, a case study was performed on a ransomware scenario.
- D4.2 (this deliverable) focuses on the refinement of the SEConomy framework by providing new use cases under investigation. Also, a SEConomy-based tool will be proposed to support cybersecurity economics quantification and related risk analysis.
- D4.3 will provide the final recommendations on the economic perspectives and discuss state-of-the-art approaches proposed to support the decision-process of investments in cybersecurity as well as to minimize the loss of business affected by cyber attacks (e.g., cyber insurance).

Overall, in Year 2, activities in T4.1, T4.2, T4.3 have been proceeding, as planned. COVID-19 pandemic has been taken into account under the respective activities and, therefore, the present deliverable encapsulates the respective output (e.g., the impact of COVID-19 on the evolving cybersecurity threat landscape. Furthermore, the impact of COVID-19 was addressed -to an extent- in the context of the interviews with CONCORDIA pilots, as this was considered relevant to capture the impact of COVID-19 on cybersecurity practices at an organizational level. From an operational point of view, the COVID-19 pandemic, however, neither affected the performance of the research activities and of other type of work, that preceded the drafting of the present deliverable nor the drafting itself of this deliverable.

[23] Notably, interviewees were informed that for the purpose of the performance of the specific interviews the Chatham House Rule would apply.

1.3. Structure of the Document

D4.2 is structured as follows: Chapter 2 presents the CONCORDIA Environment focusing on domains of interests and stakeholders. Chapter 3 presents the technological perspective of cybersecurity threats focusing on assets, emerging threats, and evolving attacks in the domains of interest of CONCORDIA. Chapter 4 captures the updates on the legal perspective along with forthcoming regulations applicable at EU level, identifies gaps and challenges at the level of implementation based on input collected through interviews and puts forth early recommendations of specific and wider relevance. Chapter 5 presents the economic perspective wherein new approaches are implemented along with case studies that have been conducted to determine their feasibility. Chapter 6 presents concluding remarks and an outlook on future work.

2. CONCORDIA Environment[24]

This Chapter presents the CONCORDIA environment and summarizes the domains of interest that are the target of the study in this deliverable and stakeholders benefiting from it. Domains and stakeholders represent the common basis linking the work in this deliverable to the effort done in WP1 and WP2, on one side, and WP4 on the other side. The Chapter summarises the related discussion under D4.1, further amending it -to an extent- for the scope and purpose of this deliverable.

2.1. Domains of Interest

Cybersecurity threats are analysed in this deliverable from different perspectives, called domains, to the aim of identifying emerging threats and attacks, as well as setting the scene for the associated implications in relation to the domains of interest of CONCORDIA. These domains, taken from the research domains of WP1 (Figure 1), are: (i) network-centric, (ii) system/software-centric, (iii) application-centric, (iv) data-centric, (v) user-centric, (vi) 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.

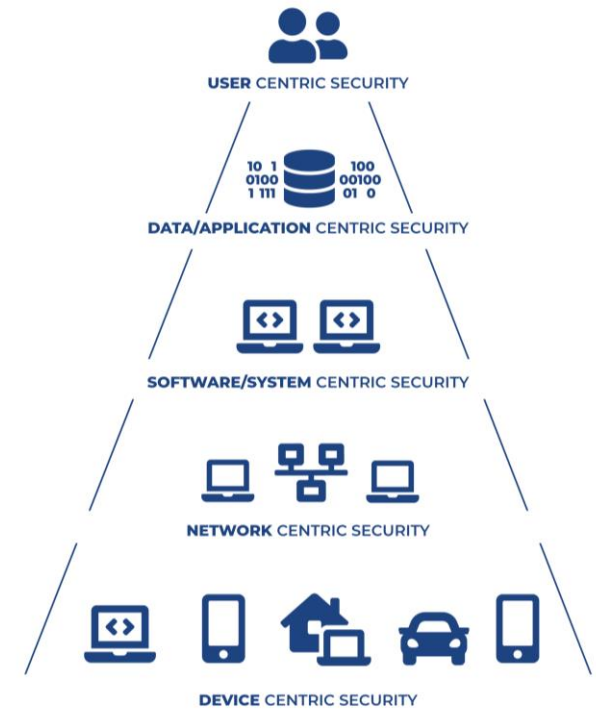


Figure 1: Domains of interest

Note that the above domains depicted in Figure 1 apply to any environments ranging from traditional distributed IT systems, to devices that produce raw data, such as embedded

[24] For consistency purposes between the three (3) consecutive deliverables, D4.1, D4.2 and D4.3 and readability purposes concerning the present deliverable, this Chapter is extracted as such from Deliverable D4.1 1st year report on cybersecurity threats.

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 microservices.

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 in the identification of 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 members of the network are European entities, Research entities, Companies, National and International entities[25] . 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 centre 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: Global Cyber Security Center (GCSEC), National Cyber security Agency of France, and National Cyber Security Centre of Lithuania. National agencies are responsible to develop and distribute awareness and knowledge on cybersecurity. They provide support to the national entities and companies on policies, regulations, and standards. National entities include Military, Navy, Healthcare sector, and Airlines. In some cases, they manage Internet operations of national entities and propose cybersecurity plans and investigate cybersecurity attacks.

[25] P. Pagani, Cyber Defense Magazine (CDM), Cyber Defense Media Group, 2019.

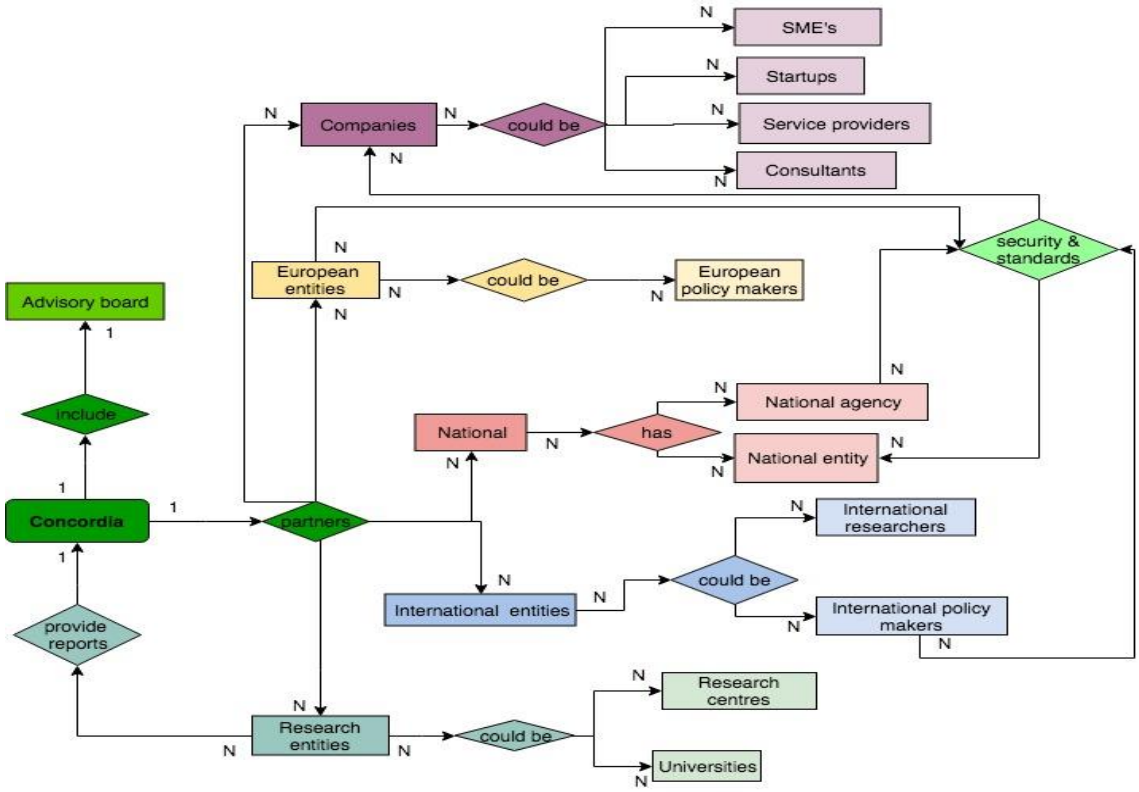


Figure 2: CONCORDIA stakeholders

As far as CONCORDIA consortium is concerned, partners are start-up companies, service providers, consultants, SME's, large multinational companies or even research entities. In particular, collaboration between companies and research entities helps companies increase their security awareness and posture but also helps the research entities gain an understanding of the concrete industry needs and requirements. Companies contribute their expertise and allow research entities to access their knowledge resources[26] [27]. Research entities can be Universities and Research centers. Center for strategic and international studies (CSIS), National Counterintelligence and Security Center (NCSC) can be the possible stakeholders. Research entities contribute and participate in the research and development process and provide reports to the CONCORDIA partners about existing solutions and increase the security awareness among them.

Furthermore, CONCORDIA interacts in diverse fora with international organizations, such as the World Economic Forum.

[26] H. Österle e B. Otto, «Consortium Research: A Method for Researcher Practitioner Collaboration in Design-Oriented IS Research,» Business & Information Systems Engineering, vol. 2, n. 5, pp. 283-293, October 2010.
[27] F. Xia, L. T. Yang, L. Wang e A. Vinel, «Internet of Things,» International Journal of Communication Systems 25 (September 2012), vol. 9, pp. 1101-1102, 2012.

3. Cybersecurity Gaps and Challenges [28]

This chapter analyses and discusses technical gaps and challenges with respect to the threats and vulnerabilities identified in D4.1, managing crosscutting aspects of the threat landscape affecting more domains of interest. In particular, we briefly introduce the overall process used in the discussion of the technical cybersecurity gaps and challenges (Section 3.1). We then present a threat map summarizing all identified threats in D4.1 and a brief overview of the COVID-19 impact (Section 3.2). We further present an update of the cybersecurity threat report, together with a throughout analysis of the gaps and challenges providing a section for each domain of interest (Sections 3.3, 3.4, 3.5, 3.6, 3.7, 3.8). We finally present a summary of our findings (Section 3.9) and the plan for additional dissemination material (Section 3.10).

3.1. Introduction

Technical aspects of D4.2 refine the threat landscape in D4.1 and focus on the gaps and challenges in the domains of interest. Activities in T4.1 built on the competences of partners in CONCORDIA, benefiting from their direct contributions. To better manage threat reporting activities, we relied on the different working groups formed in the first year, one for each domain of interest (i) Device/IoT-centric, (ii) network-centric, (iii) system-centric, (iv) data-centric, (v) application-centric, and (vi) user-centric security. The work in each working group was supervised by UMIL and coordinated by a project partner responsible for collecting relevant material and contributions from the consortium. The collected material was then analysed and prepared for the threat reporting in D4.1 and the gaps and challenges in D4.2. Each working group produced a section part of this deliverable (Section 3.3-Section 3.8), elaborating on the gaps and challenges in the areas addressed by the working group, as well as contributing to the key findings in Section 3.9, as follows.

- **Working Group 1:** "Device/IoT-centric security"
  Workgroup Chair: UMIL
  Reporting Section: Section 3.3
- **Working Group 2:** "Network-centric security"
  Workgroup Chair: TI
  Reporting Section: Section 3.4
- **Working Group 3:** "System-centric security"
  Workgroup Chair: UMIL
  Reporting Section: Section 3.5
- **Working Group 4:** "Data-centric security"
  Workgroup Chair: UMIL
  Reporting Section: Section 3.6
- **Working Group 5:** "Application-centric security"
  Workgroup Chair: ATOS
  Reporting Section: Section 3.7
- **Working Group 6:** "User-centric security"
  Workgroup Chair: UMIL
  Reporting Section: Section 3.8

[28] To the extent necessary, this Chapter has been based on the discussion linked to the Technological Perspective, as captured under Chapter 3 of Deliverable D4.1 1st year report on cybersecurity threats.

The analysis has been based on an extensive review of actual incidents and attacks presented in articles, technical blogs, conference papers, as well as online surveys for gathering supplemental information. We reviewed documents from main organizations, including for instance ENISA, CSA, IETF, OWASP, Europol and its Internet Organised Crime Threat Assessment (iOCTA).

3.2. Cybersecurity Threat Map

Drawing upon the domains of interest identified under Task 4.1, this section reports the cybersecurity threat map identified in D4.1, that is the starting point for the work on gaps and challenges in this deliverable. Table 1 summarizes the mapping between the identified threat groups, threats and the domains network, system, device/IoT, data, application, user. Table 1 specifies the threat numbering format, driving the discussion in the remaining of Chapter 3. As an example, threat T2 "Denial of Service", in threat group TG4 "Nefarious Activity/Abuse", of domain D1 "Device/IoT" is referenced in the text as T1.4.2.

Table 1: Cybersecurity threat map. Numbers in parentheses are used for threat numbering in the form T(D).(TG).(T) From D4.1.

Domain (D)	**Threat Group (TG)**	**Threats (T)**
Device/IoT (1)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)
	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (2)
	Intentional Physical Damage (3)	Device modification (1) Extraction of private information (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software/activity (3) Misuse of assurance tools (4) Failures of business process (5) Code execution and injection (insecure APIs) (6)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1)
Network (2)	Unintentional damage / loss of information or IT assets (1)	Erroneous use or administration of devices and systems (1)
	Interception and unauthorised acquisition (2)	Signaling traffic interception (1) Data session hijacking (2) Traffic eavesdropping (3) Traffic redirection (4)
	Nefarious activity/abuse (3)	Exploitation of software bugs (1) Manipulation of hardware and firmware (2) Malicious code/software/activity (3) Remote activities (execution) (4) Malicious code - Signaling amplification attacks (5)
	Organisational (failure malfunction) (4)	Failures of devices or systems (1) Supply chain (2) Software bug (3)
System (3)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)

	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (data breach) (2)
	Poisoning (3)	Configuration poisoning (1) Business process poisoning (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software/activity (3) Generation and use of rogue certificates (4) Misuse of assurance tools (5) Failures of business process (6) Code execution and injection (insecure APIs) (7)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1) Malicious Insider (2)
Data (4)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)
	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (data breach) (2)
	Poisoning (3)	Data poisoning (1) Model poisoning (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software /activity (3) Generation and use of rogue certificates (4) Misuse of assurance tools (5) Failures of business process (6) Code execution and injection (insecure APIs) (7)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1) Malicious insider (2)
Application (5)	Unintentional damage (1)	Security Misconfiguration (1)
	Interception and unauthorised acquisition (2)	Interception of information (1) Sensitive data exposure (2)
	Nefarious activity/abuse (3)	Broken authentication and access control (1) Denial of service (2) Code execution and injection (insecure APIs) (3) Insufficient logging and monitoring (4) Untrusted composition (5)
	Legal (4)	Violation of laws or regulations (1)
	Organisational threats (5)	Malicious Insider (2)
User (6)	Human Errors (1)	Mishandling of physical assets (1) Misconfiguration of systems (2) Loss of CIA[29] on data assets (3) Legal, reputational, and financial cost (4)
	Privacy breaches (2)	Profiling and discriminatory practices (1) Illegal acquisition of information (2)
	Cybercrime (3)	Organized criminal groups' activity (1) State-sponsored organizations' activity (2) Malicious employees or partners' activity (3)
	Media amplification effects (4)	Misinformation/disinformation campaigns (1)

[29] Confidentiality, Integrity, Availability (CIA)

		Smearing campaigns/market manipulation (2) Social responsibility/ethics-related incidents (3)
	Organisational threats (5)	Skill shortage/undefined cybersecurity curricula (1) Business misalignment/shift of priorities (2)

The recent ENISA Threat Landscape (ETL) 2020[30] (published on 20 October 2020) highlighted that COVID-19 led transformation of the digital environment resulting in an impact to the threat landscape. During the pandemic, cyber criminals have been seen advancing their capabilities, adapting quickly and targeting relevant victim groups more effectively. The ETL report highlights important aspects and trends related to the threat landscape that were impacted by COVID-19:

- There will be a new norm during and after the COVID-19 pandemic that is even more dependent on a secure and reliable cyberspace;
- The number of fake online shopping websites and fraudulent online merchants reportedly has increased during the COVID-19 pandemic. From copycats of popular brands websites to fraudulent services that never deliver the merchandise, the coronavirus revealed weaknesses in the trust model used in online shopping;
- The number of cyberbullying and sextortion incidents also increased with the COVID-19 pandemic. The adoption of mobile technology and subscription to digital platforms makes younger generations more vulnerable to these types of threats;
- The number of phishing victims in the EU continues to grow with malicious actors using the COVID-19 theme to lure them in. COVID-19-themed attacks include messages carrying malicious file attachments and messages containing malicious links that redirect users to phishing sites or malware downloads;
- Business Email Compromise (BEC) and COVID-19-themed attacks are being used in cyber-scams, resulting in the loss of millions of euros for EU citizens and corporations.

In this context, COVID-19 Pandemic has brought a significant increase in and worked as a multiplier of cyber-attacks. Starting from Table 1, in the following section, we report for each domain of interest: i) a summary from D4.1, ii) new threats in the pandemic era, iii) identified gaps and challenges. Finally, we present the key takeaways emerging from our analysis and an overview of dissemination documents that are under preparation.

3.3. Device/IoT-Centric Security

3.3.1. Threats (from D4.1)

We provide a summary of the threat categories identified in D4.1 in the domain Device/IoT. In general, the IoT scenario revolutionizes the concept of security, which becomes even more critical than before. Security protection must consider millions of devices that are under control of external entities, freshness and integrity of data that are produced by these devices, and heterogeneous environments and contexts that co-exist in the same IoT environment [1]. Trend Micro[31], a cybersecurity solutions provider, stated that the IoT has

[30] ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

[31] IoT Devices: A Target in Cybercriminal Underground, https://www.trendmicro.com/en_us/research/19/i/this-week-in-security-news-iot-devices-are-a-target-in-cybercriminal-underground.html

become a primary target for cybercriminals. The SonicWall 2019 report shows that IoT malware increased 55% and threats related to encryption spiked 76% compared to 2018.[32] This trend leads to an increase in budget for security in IoT. According to Gartner[33], the IoT security budget will reach $3.1 billion in 2021.
Concerning attack vectors in IoT, according to F-Secure Attack Landscape H1 2019[34], the Telnet protocol is the one mostly used among the TCP-based ones, while the UPnP is the top exploit among the UDP ones[35].
Given the peculiarity of IoT devices, which are in many cases outdated embedded systems, F-Secure estimated half a billion IoT devices vulnerable to 10-year-old vulnerabilities[36].

Even considering the heterogeneous nature of the assets belonging to the Device/IoT domain, the IETF definition of threat[37], namely, "*a potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm*", is in general enough to cover with all the IoT threats. IoT has a specific peculiarity: the strong link between security leakages and safety. ITU-T in its report Y.4806[38] underlines this link identifying a list of threats that are capable to affect safety. OWASP identifies in the 2018 the top 10 IoT security threats, where weakness of passwords, network services and interfaces are identified as the top three threats.
Our threat taxonomy is a consolidation of threats previously considered in other documents/reports[39] [40] [41] and is composed of the following groups.

- TG1.1 – Unintentional damage/loss of information or IT assets: This group includes all threats causing unintentional damage, including security, safety and information leakage or sharing due to human errors.
- TG1.2 – Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties. This TG, depending on the circumstances of the incident, can also be linked to TG5.
- TG1.3 – Intentional physical damage: in IoT the physical access to the devices that are spread in a potential uncontrolled environment, which is more serious than in another domain.
- TG1.4 – Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks, targeting the infrastructure of the victim, including the installation or use of malicious tools and software.
- TG1.5 – Legal: This group provides threats resulting from violation of laws and/or

[32] SonicWall Mid-Year update report https://www.sonicwall.com/resources/white-papers/mid-year-update-2018-sonicwall-cyber-threat-report/
[33] Gartner Says Worldwide IoT Security Spending Will Reach $1.5 Billion in 2018 https://www.gartner.com/en/newsroom/press-releases/2018-03-21-gartner-says-worldwide-iot-security-spending-will-reach-1-point-5-billion-in-2018
[34] Internet Security Glossary, Version 2, Attack Landscape H1 2019: IoT, SMB traffic abound, https://blog.f-secure.com/attack-landscape-h1-2019-iot-smb-traffic-abound/
[35] ATTACK LANDSCAPE H1 2019 https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/09/12093807/2019_attack_landscape_report.pdf
[36] F-Secure IoT threat landscape - Old hacks, new devices, https://s3-eu-central-1.amazonaws.com/evermade-fsecure-assets/wp-content/uploads/2019/04/01094545/IoT-Threat-Landscape.pdf
[37] Internet Security Glossary, Version 2, https://tools.ietf.org/html/rfc4949
[38] Security capabilities supporting safety of the Internet of things, https://www.itu.int/rec/T-REC-Y.4806-201711-I/en
[39] ENISA Smart Grid Threat Landscape, and Good practice https://www.enisa.europa.eu/publications/smart-grid-threat-landscape-and-good-practice-guide
[40] ENISA Threat Landscape and Good Practice Guide for Internet Infrastructure https://www.enisa.europa.eu/publications/iitl/at_download/fullReport
[41] ENISA Threat Landscape and Good Practice Guide for Smart Home and Converged Media https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence

regulations, such as the inappropriate use of Intellectual Property Rights, the misuse of personal data, the necessity to comply with judiciary decisions dictated with the rule of law. Section 4 of the present document will discuss aspects of this TG.

- TG1.6 – Organisational threats: This group includes threats to the organizational sphere.

We remark that botnets are a security concern, typically involving IoT, but not very often targeting IoT itself. Botnets normally exploit IoT vulnerabilities to infect the devices. Initially, IoT botnets were grounded on manual physical malicious activities on the devices (TG1.3), or on exploiting the access control weaknesses and default passwords (T1.1.1). Later, attackers focused on protocol weaknesses (TG1.2), vulnerabilities in general (TG1.4) and diffusion via malware. Recent botnets adopt hybrid approaches to infect the devices, therefore they can be associated with different threats. Next, we associate specific botnets of threat groups, considering the principal threat type used to implement the botnets. In addition, proxy threats are common, where a compromised device is used as a proxy to launch attacks, hiding the identity of the attacker. In this case, no infection is needed, just the reuse of existing functionality.

3.3.2. New Threats and COVID-19

During the pandemic, we experienced an increase in IoT device adoptions. Juniper Research predicts an increase of 20% of revenue in 2020 compared to 2019, reaching $66 billion[42]. Between the first and the second pandemic wave, when the business started to re-open safety, touchless and contactless devices such as body temperature cameras and touchless point of sales have become a necessity. IoT is also used for contact tracing, which is very useful to counteract pandemic diffusion[43] despite the privacy debate around their usage to contrast emergency situations. Medical devices are increasingly adopted due to the fact that they are equipped with remote control features. This is fundamental to preserve social distance in critical environments and offer better a more effective patients' control even in situation where the number of caregivers per patients is critically low.

Health devices suffers from the same weaknesses as any IoT devices, exacerbated by the strict relation with safety and the leakages of the working environment, which is not designed to handle networks of things.

The large adoption of remote working is another aspect that from an IoT security perspective is having serious repercussions on organizations. More specifically remote working results in the use of many personal devices to connect to the corporate network ranging from mobile phone to tablet and laptop. Such devices are not dedicated for work and share a number of other services for media, shopping and entertainment and they are typical far less protected. Such personal devices are also typically connected to less protected home network where other devices also reside, offering new possibilities for an attacker to indirectly threaten the company network. This is increasing the severity of business process threats (T1.4.5).

[42] The Internet of Things: Consumer, Industrial & Public Services 2020-2024 https://www.juniperresearch.com/researchstore/devices-technology/internet-of-things-iot-data-research-report

[43] Accent Systems developed a connected wristband technology to contain the spread of Covid-19 https://accent-systems.com/blog/accent-systems-developed-connected-wristband-technology-contain-covid19/

The fast adoption of solutions to rapidly react to an emergency, without the time for an accurate planning is exacerbating the IoT leakages. This impacts on inadequate planning threat (T1.1.2). In fact, most of the security measures and best practices that could be adopted during the design of a relevant solution, (e.g., environmental security protections, security by design etc.) were, in most of the cases, not adopted since that would require a detailed design phase. The connection first and secure later attitude, which is largely used in IoT, is always not preferable and despicable when the effort to secure later is not available due to the pandemic crisis.

The pandemic is also underlining the importance of implementing strong cyber hygiene among employees. Skill shortage is much more severe under stress (T1.6.1).

In a pandemic context, where the government imposes restrictions and there is a lack of available cybersecurity personnel, adversaries are likely to target critical infrastructure more aggressively, with fewer resources able to respond to evolving threats. In addition, vaccine makers have been identified as new sensible targets and are under an increasing pressure by a number of advanced persistent threats (APT) groups.[44]

During the pandemic we are experiencing a huge increase of internet traffic and workload, however IoT networks seem not to be directly impacted. However, they are impacted by the delay on the technological roadmap that involve them as one of the emerging technologies (e.g., 5G release 16 delayed announcements by 3GPP are very important for IoT)[45].
According to Checkpoint[46], "71% of security professionals have noticed an increase in security threats or attacks, since the beginning of the Coronavirus outbreak."[47] Even if none of them directly target IoT as devices, they can have an effect, since IoT access credentials may be leaked or smart devices at home may infiltrate corporate networks. IoT analytics also identified in the April 2020 report some positive effects of COVID-19 in IoT; that for security there is principally a better awareness on the problem[48].
According to bitdefender [49], suspicious incident reports related to IoT devices increased by 46%, from January to June 2020 (people staying home much more during the lockdown period) and ransomware 7 times more during this period.

Table 2 shows an update, with respect to D4.1, of the cybersecurity threat map in the IoT/device domain. In particular, two threats have been added as follows.

Threat T1.1.3: Inadequate design and planning or incorrect adaptation in critical scenario – COVID-19. It considers the absence or inadequacy of emergency reaction plan or adaptation strategy to new security threats derived from a fast adoption of new IoT devices

[44] The European Medicines Agency (EMA) says it has been hit by a cyber-attack and documents relating to a Covid-19 vaccine have been accessed. https://www.bbc.com/news/technology-55249353
[45] 3GPP Releases https://www.3gpp.org/specifications/releases
[46] A Perfect Storm: the Security Challenges of Coronavirus Threats and Mass Remote Working , https://blog.checkpoint.com/2020/04/07/a-perfect-storm-the-security-challenges-of-coronavirus-threats-and-mass-remote-working/
[47] A Perfect Storm: the Security Challenges of Coronavirus Threats and Mass Remote Working https://blog.checkpoint.com/2020/04/07/a-perfect-storm-the-security-challenges-of-coronavirus-threats-and-mass-remote-working/
[48] State of the IoT Q1/2020 & COVID-19 Impact: https://iot-analytics.com/product/state-of-the-iot-q1-2020-covid-19-impact/
[49] Bitdefender Mid-year Threat Landscape Report 2020: https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

and technologies to react to crisis. It is similar to the need of a disaster recovery plan, but focused on the adoption and the adaptation of security countermeasure to cope with new emerging needs.

Threat T1.3.3: Lack of control on safety implications – COVID-19. The pandemic let the connection between IoT security and safety to emerge more clearly. There is a severe risk that the new plethora of IoT medical devices that monitor conditions, even at home, constitute a serious safety threat for people. In addition, the urgency of the adoption of such devices makes any possible security/safety-oriented planning unfeasible.

Threat T1.6.2: Lack of strong cyber hygiene practices – COVID-19. Good practices that helps to improve cybersecurity skills are fundamental under any situation. With the pandemic, the personnel are exposed to stress and to adopt new technologies that they do not have time to learn how to use. In IoT this is even more severe, due to their nature to be ubiquitous and out of the box deployable. The minimal cyber hygiene practices are fundamental in such context.

Table 2: Update on cybersecurity threat map in the Device/IoT domain

Domain (D)	**Threat Group (TG)**	**Threats (T)**
Device/IoT (1)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2) **Inadequate design and planning or incorrect adaptation in critical scenario – COVID-19 (3)**
	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (2)
	Intentional Physical Damage (3)	Device modification (1) Extraction of private information (2) **Lack of control on safety implications – COVID-19 (3)**
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software/activity (3) Misuse of assurance tools (4) Failures of business process (5) Code execution and injection (insecure APIs) (6)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1) **Lack of strong cyber hygiene practices – COVID-19 (2)**

According to the IoT analytics report[50] the pandemic is also an opportunity to accelerate the security trends. Particularly, the identified five top areas of IoT security[51] are: i) holistic assent inventory management, ii) scans for shadow IT devices and strong cyber hygiene among employees, ii) review what should be in the cloud for remote management, iv) shift-left security practices[52], v) automate security effort with AI.

[50] IoT Security Market Report 2020-2025 https://iot-analytics.com/product/iot-security-market-report-2020-2025/

[51] 5 IoT Security best practices to consider after the Covid-19 lockdown https://iot-analytics.com/5-iot-security-best-practices-after-the-covid-19-lockdown/

[52] The System Sciences Institute at IBM found that addressing security issues in design was six times cheaper than during implementation. They also found that addressing security issues during testing could be 15 times costlier.

3.3.3. Gaps and Challenges

In this section we provide an overview of gaps and challenges that impact the cybersecurity IoT/device domain, discussing those scenarios where further research and investigations are required.

Initially, it aims to complete the analysis done in this section with those gaps and challenges that either affect the IoT/device domain alone, or in conjunction with other domains. Next, it provides a binding between identified threats, relevant assets and described gaps/challenges as presented in Table 3.
In a nutshell, devices in IoT are not actually capable to fully implement all the modern protection strategies and mechanisms. Actual solutions concentrated the protection on nodes showing computation capabilities (in most of the cases Edge devices and the cloud services), leaving the periphery almost unprotected, claiming that most of the sensible data resides on the central part of the IoT ecosystems. There is an obvious risk in such scenario, where the source of data (i.e., the sensors) cannot be protected and also exposed to physical attacks like substitution and cloning. These attack permits impersonification and introduces more dangerous attacks on the cloud counterpart of the IoT system. However, a direct protection to this type of physical threats is economically very expensive (e.g., TPM and cryptography) for simple devices that should costs as less as possible. In addition, IoT devices tend to be manufactured and shipped as "closed" devices, so they cannot be easily updated and patched with the same effectiveness as other systems and they are still exposed to a number of persistent threats. One effect of this situation is that the IoT systems themselves are used to generate botnet attacks.
Another aspect to be considered is the relation between the cloud and the IoT and in particular edge systems. Finding a good balance in terms of functional tasks to be executed and non-functional protection to be implemented is complex, in many situations is application specific and it generates system weaknesses. In case the IoT environment is composed of mobile devices, this relation is even more complex and dynamic, since the different devices should refer to different edges, while interacting to the cloud introducing additional risks.
Currently, IoT is becoming largely used in many critical sectors like the health, industrial manufacturing, UAV to name but a few. In these sectors many IoT are also actuators capable to actively interact with the environment and therefore their security is becoming strictly connected to human safety. On one side, his leakage is reducing the real applicability of IoTs and on the other it increases the risks.
All these weaknesses require technical and design countermeasures. Also, we note that these countermeasures cannot be just the application of traditional ones, since they are almost not applicable. A preliminary step towards this direction would be the adoption of 5G with all the security features activated as an enabler for more advanced IoT ecosystem, but currently it is still not fully implemented and adopted in concrete, and it will not be free of risks as well. Also, we note that it is required to address the dramatic skill shortage that exists in the adoption of personal IoT ecosystem, like demotics and smart devices. A peculiarity of IoT is that it is largely adopted by non-expert users unaware of the security/privacy risks they are facing.

IoT/Device Domain-Specific Gaps and Challenges

G1.1 - Gaps on design. IoT is just recently but slowly being designed, considering security as principal requirements.[53] In most of the cases IoT systems have no defence-in-depth strategy such as secure boot process isolation of a Trusted Computing Base.[54] In addition, basic good practices like the limitation of the number of open ports and the authentication, are normally not considered or are very weakly implemented. In general, the concept of security-by-design or privacy-by-design is not taken into account by most of the IoT manufacturers. In many cases information is exchanged with a third-party without the control, credentials are stored as plain text and cannot be modified (i.e. hard coded default password).

G1.2 - Gaps on protection mechanisms adoption and hardening. The current advanced protection mechanisms cannot be adopted by most of the IoT systems, due to a number of limitations including the limited computational power and the variety of communication protocols adopted. There is a clear lack of communication protection, on internal as well as external interfaces that depend on one side on the protocols used and on the other on the absence of resources to improve the protocols security. There is no data execution prevention or attack mitigation techniques implemented at firmware level. CSA released a set of recommendations to harden the firmware upgrade process in IoT, since it is perceived as a very challenging and weak part of the IoT protection [55]. Generally, there is a widespread vulnerability to persistent threats, due to a number of public well-known vulnerabilities that left unfixed and to a number of services that are exposed through different not necessary entry points. Similarly, to most of the complex architectures correct configurations are crucial in order to prevent security weaknesses. In IoT, configurations are exposed to many possible flows also due to difficulty to change and fix them.

G1.3 - Gaps on authorization and authentication. IoT systems rarely adopt advanced authentication and authorization architectures between devices. In addition, some critical tasks like firmware update can be in most of the cases executed without a signature check allowing tampering and usurpation. Similarly, in many situations, software updates are possible without authorization and file trust verification. One of the critical phases of an IoT device is the boot phase where authorization and authentication can help in hardening the device against critical threats. In many situations secure boot is not implemented. IoT is also typically exposed to risks associated to weak password policies or default passwords left unchanged.

G1.4 - Gaps on diagnosis and response capabilities. IoT devices are rarely equipped with diagnosis tools that can be used to monitor their status. In many scenarios they are not always connected to the rest of the system and their response capabilities are limited. It is in general complex to control the IoT periphery making IoT ecosystem exposed to a number of threats, including cloning and substitutions.

[53] New Security Guidance for Early Adopters of the IoT https://cloudsecurityalliance.org/download/new-security-guidance-for-early-adopters-of-the-iot/

[54] IoT Security Guidelines for Service Ecosystems http://www.gsma.com/connectedliving/wp-content/uploads/2016/11/CLP.12-v1.1.pdf

[55] Recommendations for IoT Firmware Update Processes, available at: https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/recommendations-for-iot-firmware-update-processes.pdf

G1.5 - Lack of awareness and knowledge (skill shortage). Security experts are commonly familiar with traditional IT security, but not with IoT security peculiarities. There is a lack of knowledge regarding i) the threats in IoT and how they differ from the traditional system threats and ii) the countermeasures and mechanisms to be adopted. There is also an overall lack of awareness regarding the need of security in IoT devices. Most of the IoT consumers do not have the basic understanding of their IoT devices and the impact on their environment, in terms of security and safety. This aspect may lead to devices not being updated with the consequent security weakness. Therefore, there is the need to properly train employees and educate consumers about the use and the security risk posed by IoT including safety. Also, it is becoming important to provide knowledge on how to prevent protect and react in case of security incident involving IoT. Moreover, there is a lack of awareness at societal level. End users are not well aware of the risks incurred. Cybersecurity is not widely embraced as an essential requirement in the market of IoT.

G1.6 - Lack of interoperability. Most of the IoT systems are adopted as an offshoot of a traditional ICT ecosystem. This approach and the lack of common regulations cause a number of interoperability issues between devices of different manufacturers, as well as between different security models adopted within the IoT subsystem. Therefore, it is important to ensure correct and secure interoperability, avoiding conflicts and incompatibilities that expose the entire system to security risks. An example is the proprietary protocol developed by a specific manufacturer that causes incompatibilities with others and may requires ad hoc software bridges that can be exposed to security issues. This requires the development and use of standard protocols to ensure a good level of interoperability with the least efficiency and security loss. It is a largely known good practice not to use close-source and proprietary protocols as their security cannot be verified and was proven that security through obscurity does not provide proper security coverage.
An important role is also played by frameworks. Similar to the protocols, the use of common frameworks can also help to improve the efficiency and security of the devices when interconnected for a specific application purpose.

G1.7- Lack of security-dedicated budget. IoT manufacturers tend to consider functionality more important than security, secure design and code quality. Their economic interests are not aligned with the need of security and, in some cases, they do not consider security at all. Security and code quality are in general expensive and no direct return-on-investment is perceived by the manufacturer. They are also not capable to evaluate the economic impact and perceived reputation impact of hypothetical security weaknesses. Actually, there are not economic incentives for the manufacturer to change this trend. EU level funds can play this role, but they are very competitive and most of the manufacturers does not have the necessary skills to compete on EU tender calls. It is well known that different risks and threats are usually underestimated and left out because of budgetary issues. There is a quite consolidated tendency to handle security concerns a-posteriori of incidents.

G1.8- Fragmentation in security approaches and regulations. There are actions at EU level focused on a homogeneous regulation of cybersecurity across Member States (e.g., Cybersecurity Act) but also other recently enforced regulations, like the NIS Directive, that do not guarantee the same degree of homogeneity, when it comes to the applicable regulatory frameworks and their enforcement[56]. Concerning IoT, there still an absence of

[56] Note that this is clearly reflected in the recent Report from the Commission to the European Parliament and the Council assessing the consistency of the approaches taken by Member States in the identification of

regulation addressing all the relevant aspects in an up-to-date manner, hinders both the identification of commonly accepted requirements for manufacturers, as well as the setting of clear expectations from customers. In case of a security incident, the distribution of liabilities in such scenario becomes problematic (e.g., complex Industry 4.0 scenario involving safety). A recent trend on Industrial Internet of Things IIoT is exacerbating IoT security issues and lacks on clear legislation on liabilities distribution. IIoT is in its infancy, is a multidisciplinary application area by definition and an initial effort in sharing common taxonomy is just recently released by CSA.[57]
There are some generic recommendations released even in early 2015[58] but a mature security framework still missing. CSA released in 2019 its control framework[59], but still not assimilated by all the actors involved. Most of companies and manufacturers are taking their own approach when implementing security. This results in a lack or slow embracement of standards to guide a security aware IoT adoption.
A key to rapid progress in this context is to get the public and private sectors to work together and understand that security is shared responsibility that involves everyone from the manufacturer to the customer or IT professional.
The fragmentation of the regulations also poses a barrier in IoT adoption in critical ICT scenarios where traditional ICT is extended with IoT layers. There is no unique and clear regulation on security measures and protocols to be used at different levels of an IoT ecosystem, making integration of safety and security much more complex. In addition, even if good practices for ICT development exist, like DevSecOps and some recommendations on how to embed security and safety in the IoT development lifecycles, they are not mature enough to cope with all the peculiarities of IoT. An important aspect to be considered is the different application areas where IoT systems are adopted. It is very complex to have a one-size fits all standards across all the IoT ecosystem. Different application areas have diverse security requirements and different constraints on the IoT ecosystem.

G1.9- Product lifecycle management leakages. IoT comprises such a variety of products that are in most of the cases exposed to internet and if left unattended, make the entire system surface exposed. The principal causes are the lack in lifecycle management and particularly in post deployment management such as timely patching and updating of new continuously discovered vulnerabilities.
IoT products will have to evolve in a secure way to consistently provide the solution for which they were created through their whole lifecycle. This process should involve all the actors that are in the position to implement changes needed to improve security in a cost-efficient manner. On one side the manufacturers should propose such new features but on the other organizations and users should accept the cost increase and recognize the value of security. In addition, it should be clear that such lifecycle management will impose restrictions on IoT and the related networks in order to protect patching and upgrade procedure and replace working devices that cannot be upgraded.

operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU on security of network and information systems, available at: https://ec.europa.eu/digital-single-market/en/news/report-assessing-consistency-approaches-identification-operators-essential-services

[57] Cloud Industrial Internet of Things (IIoT) – Industrial Control Systems Security Glossary, available at: https://cloudsecurityalliance.org/artifacts/cloud-industrial-internet-of-things-iiot-industrial-control-systems-security-glossary/

[58] Security Guidance for Early Adopters of the Internet of Things (IoT), available at: https://downloads.cloudsecurityalliance.org/whitepapers/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things.pdf

[59] Guide to the CSA Internet of Things (IoT) Security Controls Framework, available at: https://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework/

The deployment phase of the IoT device lifecycle is quite crucial even if it happens once per device in most of the cases. Recommendations should be followed, otherwise permanent weaknesses can be introduced in the system such as wrong configurations, absence of security features. Monitoring is one of this security features that is becoming important especially in relation to the possibility to follow post deployment lifecycle.

Gaps and Challenges in the Era of COVID-19

Similarly, to the discussion we had on the impact of COVID-19 on cybersecurity threats, COVID-19 also impacts on the gaps and challenges, changing their prioritization on one side and adding some more gaps and challenges on the other side. Regarding the prioritization of gaps and challenges, the advent of COVID-19 gave a boost to gaps G1.1, G1.6, and G1.7. The need of a rapidly adoption of new devices and technologies supporting the pandemic restrictions is exacerbating the gap (G1.1) on the application of a security by design approach. The same gap is even more exacerbated when such adoption involves critical environment, such as hospitals where also gaps on interoperability among different systems (G1.6) and the need to dedicate a budget on security (G1.7) also applies to IoT systems. Another gap that is currently much more severe due to pandemic is G1.9 on the lifecycle management. There is a clear need to be capable to manage every device remotely to cope with motion restrictions and to be capable to handle multiple fundamental devices (e.g., respirators) without entering in infected areas.

Regarding gaps and challenges, one additional emerges due to COVID-19 as follows.

G1.10 - Gaps in cyber hygiene practices. The advent of COVID-19 exposed personnel to stress the need to rapidly adopt new technologies that they do not have time to learn about. In IoT this is even more severe, due to their nature to be ubiquitous and out of the box deployable. The current practices to cope with the minimal cyber hygiene education is not enough and most of the time not capable to be offered prior to be exposed to risks. This is also connected to the skill shortage gap, affecting the learning procedure.

G1.11 - Gaps in handling critical scenarios. The pandemic let the connection between IoT security and safety emerge more clearly. The increase of IoT device adoption in critical scenarios without an emergency reaction plan or adaptation strategy is exposing people to data breaches and safety implications.

Cross-Cutting Gaps and Challenges

Today IoT ecosystem is becoming stratified in different layers showing an increasingly complex architecture. A weakness on one of these layers may impact the security of the entire system. IoT can be seen as one of these layers where weaknesses have a great impact on the rest of the system, since it is not really isolated from the rest, like in the case of virtualization and containment layers.

IoT is becoming a crucial asset to collect data and to control the environment in many critical scenarios like the Industry 4.0 and health scenarios and the UAV. In such scenarios it has to be considered as the riskiest layer. One of the challenges is how to establish a reliable trust in IoT where devices can be cloned and substituted, and data collected maliciously modified to obtain an advantage or to tamper the entire system. Trust in IoT is fundamental for every application scenario and has to be based on solid methodology. IoT weaknesses are normally exploited to tamper the centralized cloud system, thanks to the lack of a strong authentication and authorization mechanisms in IoT.

On a different perspective, IoT is also used as an asset to set up DDOS attacks to the target system using bot strategy. This peculiarity of IoT, including commercial IoT solution form domestic automation, smart TV etc., is bringing a different challenge for security which is to protect the system to be used as a source of threat for another system and not for itself. This is an evolution of traditional zombie agents used to infect PCs on a larger scale and on almost unprotected devices.

Considering to the gaps identified in this section, most of them are clearly referring to Device/IoT peculiarities only. However, they can be also considered in a more generic sense. In this case, for instance the **regulatory fragmentation** is a clearly horizontal gap that impact all the domains of interest. Similarly, the **protection mechanisms adoption and hardening**, clearly points to the need of system hardening and protections to be applied in application and networks. Most of the other gaps are also connected to networking devices that are often close to the concept of IoT device. For instance, **authorization and authentication** are two concepts that are normally not sufficiently considered in some networking protocol and peripheral devices such as Access Points. Similarly, the need of monitoring of such devices underline the gaps on their **diagnosis and response capabilities.**

Table 3 shows how gaps in the data domain affect the other domains of interest of CONCORDIA.

Table 3: Cross-Cutting Gaps

Gaps	**Additional Domains**
G1.1 - Gaps on design	System
G1.2 - Gaps on protection mechanisms adoption and hardening.	System, Application, Network
G1.3 - Gaps on authorization and authentication.	Network
G1.4 - Gaps on diagnosis and response capabilities.	Network
G1.5 - Lack of awareness and knowledge (skill shortage).	-
G1.6 - Lack of interoperability	System
G1.7 - Lack of security-dedicated budget.	-
G1.8- Fragmentation in security approaches and regulations.	all
G1.9- Product lifecycle management leakages.	System, Network
G1.10-Gaps in cyber hygiene practices	all
G1.11 - Gaps in handling critical scenarios	-

Table 4 provides a binding between identified threats, relevant assets and gaps/challenges in this section.

Table 4: Mapping Assets, Threats and Gaps

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	G1.7
	Inadequate design and planning or incorrect adaptation (2)	Device, Infrastructure, Platform and backend, Management	G1.1 G1.7

	Inadequate design and planning or incorrect adaptation in critical scenario – COVID-19 (3)		G1.1 G1.10 G1.11
Interception and unauthorised acquisition (2)	Interception of information (1)	Device, Infrastructure, Security mechanisms	G1.3 G1.6
	Unauthorised acquisition of information (2)	Device, Infrastructure, Platform and backend	G1.3 G1.11
Intentional Physical Damage (3)	Device modification (1)	Device, Infrastructure	G1.4 G1.7
	Extraction of private information (2)	Device	G1.2
	Lack of control on safety implications – COVID-19 (3)		G1.2 G1.7
Nefarious activity/abuse (4)	Identity fraud (1)	Device, Infrastructure, Platform and backend	G1.3
	Denial of service (2)	Device, Infrastructure, Security mechanisms, Platform and backend	G1.1 G1.11
	Malicious code/software /activity (3)	Device, Infrastructure, Security mechanisms, Platform and backend	G1.2 G1.9
	Misuse of assurance tools (5)	Data, Devices, Platform and backend, Infrastructure, Security Mechanisms, Management	G1.1 G1.7 G1.9
	Failures of business process (6)	Devices, Platform and backend, Infrastructure, Security Mechanisms, Management	G1.4 G1.6 G1.8
	Code execution and injection (insecure APIs) (7)	Platform and backend, Security Mechanisms, Management.	G1.2 G1.9
Legal (5)	Violation of laws or regulations (1)	all	G1.6 G1.8
Organisational threats (6)	Skill shortage (1)	Roles	G1.5) G1.7
	Lack of strong cyber hygiene practices – COVID-19 (2)		G1.7 G1.10

3.4. Network-Centric Security

3.4.1. Threats (from D4.1)

In this section we provide a summary of the threat categories identified in D4.1 in the domain network. For several years now, vulnerable network assets have been exploited as preferred targets for cyberattacks. Malicious cyber actors often target network devices, and, once on the device, they can remain there undetected for long periods. After an incident, where administrators and security professionals perform forensic analysis and recover control, a malicious cyber actor with persistent access on network devices can reattack the recently cleaned hosts. The adoption of a security assurance process that covers the entire life cycle management starting from secure design, secure development, secure deployment, security monitoring and security management is necessary to counteract these attacks. Also there are cases where attackers do not need to compromise their intended target directly but can achieve their aim by compromising its supply chain where it is least secure. In the last years there was in fact an increase in breaches caused by vulnerable software. Any given software stack can contain many sources of components and libraries in differing versions, increasing the need to assess, test and patch carefully. This threat highlights the importance of managing the supply chain.

Another source of well-known network breaches is the use of legacy protocols. Signalling exchange is required to establish and maintain a communication channel or session on telecommunication networks as well as allocate resources and manage networks. For example, 2/3G networks used Signalling System 7 (SS7) and SIGnalling Transport (SIGTRAN)[60] while 4G relies on Diameter[61]; all generations use Session Initiation Protocol (SIP) and GPRS Tunnel Protocol (GTP). Many fundamental services, such as short messaging service (SMS), are managed by these protocols. Many of these signalling protocols are outdated and have been implemented under a trust model that assumes well-behaved mobile operators without the need to deploy strong security controls.
In addition, another type of attack vector comes from flaw in the specifications. The paper in [2] is an example of vulnerabilities discovered during a careful analysis of LTE access network protocol specifications and a demonstration of how those vulnerabilities can be exploited using open-source LTE software stack and low-cost hardware. The paper in [3] demonstrates instead the usefulness of adopting formal verification tools to automatically check whether the desired security properties are satisfied or if instead the defined protocols/procedures suffer from ambiguity or under-specification.
To complete our overview of the attack scenario, another vector comes from poor configuration of network nodes as highlighted in [4].
In the following section, the most relevant network threats are reported according to the following groups.[62] [63]

- TG2.1: Unintentional damage/loss of information on IT assets: this group includes all threats causing unintentional information leakage or sharing due to human errors.
- TG2.2: Interception and unauthorised acquisition: this group includes any attack, passive or active, where the attacker attempts to listen, intercept or re-route traffic/data. An example is the man-in-the-middle attack. This group also includes manipulation attacks where the attacker attempts to alter or interfere with data in transit, in particular with signalling messages and routing information.
- TG2.3: Nefarious activity/abuse: this group includes threats coming from nefarious activities. It requires active attacks targeting the network infrastructure of the victim.
- TG2.4: Organisational threats: this group includes threats to the organizational sphere.

3.4.2. New Threats and COVID-19

COVID-19 has changed the way the world operates, the way we communicate, the mode of doing business and the functioning of governments. One effect of this massive digital adoption was an increase in cyber-attacks, which demonstrate once again the urgency and need of a secure and reliable cyberspace. Network is one of the main key assets that must assure the quality and robustness of the communication to permit citizen to follow their activities also staying at home: smart working, e-learning and other electronic services just to preserve safe the transport means.

[60] https://www.enisa.europa.eu/publications/signalling-security-in-telecom-ss7-diameter-5g/at_download/fullReport
[61] https://www.gsma.com/membership/wp-content/uploads/2018/09/Diameter-2018-eng.pdf
[62] Mobile Telecommunications Security Threat Landscape, GSMA, January 2019 https://www.gsma.com/aboutus/resources/mobile-telecommunications-security-threat-landscape
[63] Threat Landscape 2018, ENISA https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape

As also highlighted by the recent ENISA Threat Landscape (ETL) 2020[64] (published on 20 October 2020), COVID-19 led transformation of the digital environment resulting in an impact to threat landscape. During the pandemic, cyber criminals have been seen advancing their capabilities, adapting quickly and targeting relevant victim groups more effectively.

In the network domain, COVID-19 pandemic has led to:

- A spike in cyber threats that exploit telework technologies and remote tools. There is general exploitation of applications used for teleworking applications, including video conferencing software and voice over Internet Protocol (VOIP) conference call systems. Malicious cyber actors are looking for ways to exploit telework software vulnerabilities in order to obtain sensitive information, eavesdrop on conference calls or virtual meetings, or conduct other malicious activities. Malicious cyber actors may target communication tools (VOIP phones, video conferencing equipment, and cloud-based communications systems) to overload services and take them offline or eavesdrop on conference calls. Cyber actors have also used video-teleconferencing (VTC) hijacking to disrupt conferences by inserting pornographic images, hate images, or threatening language. Some telework software allows for remote desktop sharing, which is beneficial for collaboration and presentations; however, malicious cyber actors historically have compromised remote desktop applications and can use compromised systems to move into other shared applications.
- An impact on security operations (SOC) and processes due to the increased remote workforce, the disparate managed and unmanaged endpoints, the increased complexity in performing patching and hardening/upgrading and a change in network traffic baseline.

Table 5 below shows an update with respect to D4.1 of the cybersecurity threat map in the network domain. Two threats have been added as follows.

Threat 2.3.6: Exploitation of vulnerabilities in services and remote tools -COVID-19. With the increase of remote workers during the COVID-19 period, many users no longer relied on the infrastructure monitored by the company to access sensitive information on the network. Malicious cyber actors are taking advantage of this mass move to telework by exploiting a variety of publicly known vulnerabilities in VPNs and other remote working tools and software. In several examples, CISA and NCSC have observed actors scanning for publicly known vulnerabilities in Citrix. Citrix vulnerability, CVE-2019-19781 and its exploitation have been widely reported since early January 2020. Similarly, known vulnerabilities affecting VPN products from Pulse Secure, Fortinet, and Palo Alto have been exploited. The surge in teleworking has also led to an increase in the use of Microsoft's Remote Desktop Protocol (RDP). Attacks on insecure RDP endpoints (i.e., exposed to the internet) are widely reported online and recent analysis has identified a 127% increase in exposed RDP endpoints [https://us-cert.cisa.gov/ncas/alerts/aa20-099a].

Threat 2.5.1: Physical attack - COVID-19. Conspiracy theories around 5G and health have been circulating in Europe for the past 18 months or so but has recently morphed into claims that COVID-19 is being caused by 5G [https://www.bbc.com/news/av/stories-53285610].

[64] ENISA Threat Landscape 2020: Cyber Attacks Becoming More Sophisticated, Targeted, Widespread and Undetected, https://www.enisa.europa.eu/news/enisa-news/enisa-threat-landscape-2020

Base station attacks have increased due to disinformation around 5G. There have been several attacks on base stations around the world, including cables being hacked out of the masts through to petrol being poured in and around the equipment and then being set alight. The UK has appeared to be a target of these attacks with occurrences across the country. Other examples include New Zealand, The Netherlands and Ireland. The attacks on the base station have impacted the resilience, availability, and business continuity of services of the mobile networks. We note that this threat also introduces a new threat group TG2.5 Intentional Physical Damage.

Table 5 shows an update with respect to D4.1 of the cybersecurity threat map in the network domain. Please note that two threats have been added.

Table 5: Update on cybersecurity threat map in the network domain

Domain (D)	**Threat Group (TG)**	**Threats (T)**
Network (2)	Unintentional damage / loss of information or IT assets (1)	Erroneous use or administration of devices and systems (1)
	Interception and unauthorised acquisition (2)	Signaling traffic interception (1) Data session hijacking (2) Traffic eavesdropping (3) Traffic redirection (4)
	Nefarious activity/abuse (3)	Exploitation of software bugs (1) Manipulation of hardware and firmware (2) Malicious code/software/activity (3) Remote activities (execution) (4) Malicious code - Signaling amplification attacks (5) **Exploitation of vulnerabilities in services and remote access infrastructure - COVID-19 (6)**
	Organisational (failure malfunction) (4)	Failures of devices or systems (1) Supply chain (2) Software bug (3)
	Intentional Physical Damage (5)	**Physical attack – COVID-19 (1)**

3.4.3. Gaps and Challenges

This section reports an overview of the main gaps and challenges that impact the cybersecurity network domain, discussing those scenarios which require further research or a different approach to address a ‘secure by design’ network. To sum up, the results of the analysis highlights mainly the missing or at least immature level of proper security processes such as PSIRT (Products Security Incident Response Team), hardening and patching, issues related to legacy protocols still in use and other emerging threats related to new business model for Telco (e.g., IoT).

Network Domain Specific-Gaps and Challenges

G2.1 - Gaps on security testing, on security accreditation schemes of network devices and on massive deployment of PSIRT program from vendors. New/next generation networks will increasingly rely on software, virtualization and IT systems in general. To identify possible misbehavior or erroneous security configuration, that could be exploited to gain unauthorized access to a system (and then to a network), basic security and authentication schemes should be adopted on a large scale, to assess the security

requirements and functions of network devices as well as their security hardening and configurations.
The security accreditation schema should also address the secure software life cycle (security by design and testing), since software, and virtualization, are increasingly used.

As part of the security accreditation of network devices, or in addition, vendors shall offer a Product Security Incident Response Team (*PSIRT*) program to help their customers in addressing the security of their products in a prompt and efficient way. PSIRT is a dedicated service that manages the receipt, investigation, and public reporting of security vulnerability information related to products and networks, with the goal to advise in a prompt way the affected customers, helping them to resolve the newly discovered security issues.
In this way the time window of exposure to the risks associated with the possible exploitation of new vulnerabilities is significantly reduced.
As a matter of fact, many vendors are already implementing their own PSIRT processes, but such processes are generally differently implemented by each company without common standardized procedures and have to be better integrated into the Telco internal processes in charge to manage such threats communications. At the present time the Telcos, usually implementing and managing multivendor and multi technology networks, are puzzled by various source of information, usually manually managed (PSIRT communications comes in txt, PDF, excel format), resulting in unnecessary overwork and, consequently, exposing the integrity of the systems to unmanaged threats.

G2.2 - Gaps on continuous hardening & patching of IT systems. The operations and maintenance of network devices relies on IT systems, which if not properly managed from a security point of view (like for example in terms of regular patching, hardening, updates…) can be potentially abused to compromise the normal operations.
In this sense also, the Personal Computers of employers can represent a way to gain unauthorized and privileged access to the network: improvements in the security research to detect 0-day exploit as well as in preventing persistent advanced attacks, can be valuable to increment the robustness of end point systems. Given the huge number of vulnerabilities, many kinds of software updates that actually are released every day, it should be needed to patch/update the network devices continuously. Moreover, such updates, given both the number of impacted devices and the sensitivity of the provided services (e.g., connectivity, VoIP, security), are actually difficult to implement in a timely fashion, again exposing the entire system to security threats. Possible solutions should foresee automatic tools, able to help operational people to select which software update, on which device and also when (best time) install.

G2.3 – Gaps on security training and awareness toward employees. Sometimes phishing email or social engineering attacks represent the first step to gain access to a network or systems.

Artificial intelligence or *machine learning techniques* can help to complement the security awareness of employees, 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. Anyway, as we know, the human beings are usually the weakest element of the chain, and continuous security training must be considered always as a must, not only for the employee, but also for the end users of the Telco services: their devices are directly interconnected to

the access networks of the provider and if not properly managed, can be used against the Internet services (e.g. botnet launching DDos attacks against the DNS infrastructure).

G2.4 - Gaps on massive deployment of mobile signaling firewalling solutions and anomaly detection systems specific to mobile signaling protocols. To hinder the lack of security mechanisms of signaling protocols, like Signaling System 7 (SS7) and Diameter used in mobile networks, in the last few years a lot of effort was dedicated by the industry to elaborate mobile signaling firewall specification. Adversaries could exploit signaling system vulnerabilities to redirect calls or text messages (SMS) or data sessions. The adoption of firewalling techniques and of related guidelines for their configurations and the continuous improvements of the industry to increase their strength in identifying and preventing attacks, can help against Interception and unauthorized acquisition threats.
Real attacks [65] demonstrate that the need of such firewall systems is real. New implementations, e.g. 5G, have to implement signaling firewalling since the design phase.

G2.5 – Gaps on the standardization process to include formal security verification and security assessment/testing of new protocol/network specifications. Security researchers are increasingly adopting formal verification algorithms and methods to prove the security of protocols, to identify possible security issues for example in the specification of the state machine of a device or in the flow of protocols etc.
In the same way, these formal security verification methods and schemas should be adopted by the specification and standardization agencies, in order to identify and address possible security issues since the initial steps of the definition. Such issues can come, for example, from unclear specifications, or from the leak of implementation guidelines and have to be identified and removed before the official approval of a new specification.
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.

G2.6 – Gaps on best practice to increment GTP security assessment procedure and on robust solution against Data session hijacking. Recently, some paper pointed out weaknesses of protocol or of their configuration (like for example of GTP protocol[66]) that could be exploited to perform data session hijacking.
This is a critical issue since data sessions are established for every connection nowadays, so research to identify new solutions against data session hijacking can be of value to safeguard the security of users and their privacy. Some mobile operators are still exposed to vulnerabilities in the GTP protocol, opening the door to several kind of attacks, such as to denial-of-service attacks, impersonations and fraud. The issue can impact also 5G whenever "legacy" core technologies are used, in particular during the first deployments when Evolved Packet Core is still used. It is important to follow the GSMA FS.20 GPRS Tunnelling Protocol (GTP) Security recommendations to limit the exposure to such a threat.

[65] See SS7 Vulnerabilities & Attack exposure report, available at: : https://www.gsma.com/membership/wp-content/uploads/2018/07/SS7_Vulnerability_2017_A4.ENG_.0003.03.pdf , and ENISA Signalling Security in Telecom SS7/Diameter/5G, available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwjJvomUpIHrAhXhIMUKHcQVC64QFjAAegQIAhAB&url=https%3A%2F%2Fwww.enisa.europa.eu%2Fpublications%2Fsignalling-security-in-telecom-ss7-diameter-5g%2Fat_download%2FfullReport&usg=AOvVaw0aoUmR313Yc0wc-deyIusB
[66] See https://positive-tech.com/storage/articles/gtp-2020/gtp-2020-eng.pdf

G2.7 – Gaps on the deployment of robust crypto algorithms to cypher user plane traffic while minimizing performance impact and interoperability issues. User data have to be safeguarded against interception or manipulation. In this context crypto algorithms shall be applied to protect data planes.
Some gaps are related to the leak of activation of robust algorithms that are already available: it may be due for example to possible miss-configuration in commercial networks.
However, improvements in security research and attack as well as in computational resources can exploit crypto algorithms that were considered robust in the past.
So, improvements in the research to develop new crypto algorithms to protect user data, while it minimizes the performance impact will make a great difference in safeguarding user privacy.

G2.8 – Gaps on robust and innovative solution to protect DNS traffic system. DNS is at the core of the Internet and is, at the same time, one of the most sensitive services and one of the main targets for cyberattacks since DNS is actually weak in its design. Telcos and ISP are spending a lot of resources to protect their DNS infrastructures in terms of both, security technologies (firewall, IDS, monitoring tools) and security personnel. At the same time DNS-SEC, although available since the end of 90', is not widely adopted. Hence DNS remains one of the weakest services of cyberspace.

G2.9 – Gaps on wide adoption of integrity protected firmware also in IoT system Software integrity is the key to the security of the devices. Many mechanisms are available to protect the integrity of operating systems of both end user devices (e.g., PC or workstation, mobile phone) and network devices such as routers or other core elements. Although specific technology is already available, many vulnerabilities are continuously discovered (e.g., the Cisco Secure Boot[67]). Whereas traditional network elements can be managed by security personnel, IoT devices, once massively deployed, become out of range of the traditional management tools and hence the target of cyberattacks. Innovative yet simple (e.g., economic) solutions have to be defined to solve this gap, especially for low-end IoT devices.

G2.10 – Gaps on malware detection solution. According to recent security reports, malicious software (malware) is increasing at an alarming rate, and some malware can hide in the system by using different obfuscation techniques. Recently, there have been several studies on malware detection approaches. However, the detection of malware remains problematic. Signature-based and heuristic-based detection approaches are fast and efficient to detect known malware, but especially signature-based detection approaches have failed to detect unknown malware. On the other hand, behaviour-based, model checking-based, and cloud-based approaches perform well for unknown and complicated malware; and deep learning-based, mobile devices-based, and IoT-based approaches also emerge to detect some portion of known and unknown malware. However, no approach can detect all malware in the wild. This shows that to build an effective method to detect malware is a very challenging task and there is a huge gap for new studies and methods.

G2.11 – Gaps on containing amplification attacks. An Amplification Attack is aimed to cause denial of service and is based on an amplification factor to multiply the power of the attackers. Amplification attacks techniques permit a relatively small number of nodes, even with a low level of resources to generate a huge number of messages towards the target

[67] See https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190513-secureboot

victim. Signalling amplification attacks include Smurf Attacks (ICMP amplification) and in particular DNS and NTP Amplification attacks. Protection against such kind of attacks is still difficult, as also reported recently by the FBI[68] and additional research and tools have to be defined. Moreover, increasing the Threat Information sharing among organizations could help in protecting network infrastructures. Inside CONCORDIA the T3.2 (Piloting a DDoS Clearing House for Europe) and T3.1 (Building a Threat Intelligence for Europe) can actually explore the matter and propose possible mitigation means.

Gaps and Challenges in the Era of COVID-19

Regarding gaps and challenges, additional two are emerging due to COVID-19 as follows.

G2.12 – Gaps on general misinformation campaigns and Conspiracy theories. The COVID-19 pandemic has been described as a 'perfect storm' for the creation and dissemination of disinformation (intentionally misleading), misinformation (unintentionally misleading) and conspiracy theories.
The fear and anxiety created by a serious and the unexpected health threat, combined with the isolation imposed by travel and work restrictions and consequent reliance on online platforms for social interaction, have left many people vulnerable to any type of messages.
Opposition to 5G started with environmental and other groups raising concerns about health. It echoed earlier movements going back to the rollout of 3G and 4G networks, warning of long-term effects of radiation on the human body. Anonymous social media accounts have mainly been responsible for the spread of fake news exploiting fear and by using sophisticated psychological tactics (e.g., confirmation bias).
This problem points to the need to combat fake news and disinformation campaigns together with an inadequate understanding of the threats. As a matter of fact, little evidence exists linking cell phone radiation to health problems, as the World Health Organization underlines in its evaluation: "*To date, and after much research performed, no adverse health effect has been causally linked with exposure to wireless technologies," it said, adding that "so far, only a few studies have been carried out at the frequencies to be used by 5G*."[69].
COVID-19 has shown a spotlight on the role of social media in influencing political and policy debates and raised challenging questions about the need for a radical rethink of digital platform regulation. Digital platforms are ideally placed to facilitate the dissemination of disinformation and conspiracy theories and act to reinforce existing beliefs within established networks of like-minded people, due to their echo chamber effect, their lack of transparency, the ease of circulation of messages and difficulties in tracking original sources and verifying claims. Social media companies have to be more vigilant and for these reasons the mainstream platforms, such as Facebook and Twitter, have been put under pressure to remove content deemed to be against the public interest. But these efforts have limited impact as proponents of misinformation and conspiracy theorists have migrated onto other less scrutinised platforms or used coded phrases and dog whistle messaging to evade detection.

G2.13 – Gaps on reduced capacity to perform security operations. The large-scale migration to remote work, triggered by the COVID-19 pandemic increased the multiple

[68] Cyber Actors Exploiting Built-In Network Protocols To Launch Larger DDOS Attacks https://www.cyber.nj.gov/alerts-advisories/cyber-actors-exploiting-built-in-network-protocols-to-launch-attacks

[69] Additional information is available at: https://www.who.int/news-room/q-a-detail/radiation-5g-mobile-networks-and-health

challenges that security operations teams are facing in the management and capacity to perform security operations such as a reduced ability to patch and harden corporate computers that are not connecting to the company LAN, as well as a substantial decrease in the level of visibility SIEM and SOC have over user endpoints connected in remote. The implication is that they are not subject to the same level of monitoring as when directly connected to the corporate LAN, thereby reducing the overall level of security a corporate can rely on.
During COVID-19, SecOps teams face several constraints on their working practices, reduced access to operational tools. These demonstrate the need for more automation in security operations, including tools for automating protection, detection and response strategy. By automating Advanced Threat Protection, it can be possible to have real-time threat intel, which can help identify threats, combined with intelligent response to stop those threats in real-time. Proactive threat research and automated event correlation can prevent the exploitation of new avenues of attack. For example, machine learning solutions can capture IOCs (indicators of compromise) such as malicious IP addresses, domains, and URLs. And by combining machine learning with AI capabilities, those systems can also be able to continually assess new files, web sites and network infrastructures. This allows the identification of malicious components of cybercrime, as well as dynamical generation of new threat intelligence that enables to even predict and prevent future cyber threats.

Cross-Cutting Gaps and Challenges
Although current and even more future networks (e.g., 5G, but particularly 6G) are based on the availability and elaboration of huge amounts of data, networks remain the media that permits all the communications and services. If the networks fail, all the stack collapses. Actually, IoT devices, cloud services or any other layer above are based on the availability of a "network connection". The gaps identified are directly related to the network layer, but at the same time they also impact the security of the other domains.
Looking at Table 6 patching and continuous hardening remains one of the most important things to secure a system, a device, an application and a network asset so it represents a common "requirement" for most domains. Although applying patches may be a basic security principle, it's not always easy to do in practice for a number of reasons. Patching takes time and costs money. It requires to test the patches before rolling them out. It might not always be possible to patch when a system is old enough that no longer receives security updates. Also patching can be applied when you know that a vulnerability exists. This relates to another cross-cutting challenge, that is the need to promote and increase security incident response team (PSIRT) and dedicated to managing reporting of vulnerabilities in system/application/device and network product. A system that is exploited due to a vulnerability, is no longer reliable and it can compromise a network operation, it can expose data to manipulation and leak to unauthorised destinations. Each of these domains should ensure an adequate level of security and a variety of security controls including processes for secure design, development, security testing, secure operation and regular reviews of the effectiveness of all these security controls. Controls, such as security tests and compliance tests can objectively measure and reflect the level of security provided. Table 7 shows where gaps in the Network domain affect other domains of interest of CONCORDIA.

Table 6: Cross-Cutting Gaps

Gaps	Additional Domains
G2.1 - Gaps on security testing, on security accreditation schemes of network devices and on massive deployment of PSIRT program from vendors.	IoT/Device, System, Application

G2.2 - Gaps on continuous hardening & patching of IT systems	IoT/Device, System, Application
G2.3 – Gaps on security training and awareness toward employees	User, IoT/Device
G2.4 - Gaps on massive deployment of mobile signalling firewalling solutions and anomaly detection systems specific to mobile signaling protocols	-
G2.5 – Gaps on the standardization process to include formal security verification and security assessment/testing of new protocol/network specifications.	IoT/Device, System, Application
G2.6 – Gaps on best practice to increment GTP security assessment procedure and on robust solution against Data session hijacking (ie. by means of artificial intelligence systems)	-
G2.7 – Gaps on the deployment of robust crypto algorithm to cypher user plane traffic while minimizing performance impact and interoperability issues	All
G2.8 – Gaps on robust and innovative solution to protect DNS traffic system.	-
G2.9 – Gaps on wide adoption of integrity protected firmware also in IoT system	IoT/Device
G2.10 – Gaps on malware detection solution	IoT/Device, System, Application
G2.11 - Gaps on containing amplification attacks.	System, Application
G2.12 – Gaps on general misinformation campaigns and Conspiracy theories	User
G2.13 – Gaps on reduced capacity to perform security operations.	Device/Iot, System, User, Application

Table 7: Mapping Assets, Threats and Gaps

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	Core Network, Access Network, Infrastructure Network, Peering Points	G2.2 G2.3
Interception and unauthorised acquisition (2)	Signaling traffic interception	Core Network, Peering Points	G2.4 G2.5
	Data session hijacking	Core Network, Peering Points	G2.6
	Traffic eavesdropping	Radio Access Network, Infrastructure Network	G2.7
	Traffic redirection	Access Network, Core Network	G2.8
Nefarious activity/abuse	Exploitation of software bugs	Access Network, Core Network, Infrastructure Network, Endpoint Network	G2.5
	Manipulation of hardware and firmware	Core Network, Infrastructure Network, Endpoint Network	G2.9
	Malicious code/software/activity	Core Network, Endpoint Network	G2.10 G2.12
	Remote activities (execution)	Core Network	G2.2
	Malicious code - Signalling amplification attacks	Access Network, Radio Access Network, Core Network	G2.13
	Exploitation of vulnerabilities in services and remote access infrastructure -COVID-19	Access Network	G2.2 G2.12
Organization (failure malfunction)	Failures of devices or systems	Access Network, Core Network, Infrastructure Network	G2.1
	Supply chain	Infrastructure Network	G2.1

	Software bug	Access Network, Core Network, Infrastructure Network	G2.1
Intentional Physical Damage	Physical Damage – COVID-19	Access Network	G2.11

3.5. System-Centric Security

3.5.1. Threats (from D4.1)

In this section we provide a summary of the threat categories identified in D4.1 in the domain system. CSA in its "Top Threats to Cloud Computing: The Egregious 11" of the 2019, surveyed industry experts on security issues in the cloud industry, in order to rate 11 salient threats, risks and vulnerabilities. The most prominent outcome is that, compared to the previous CSA report, traditional cloud security issues under the responsibility of cloud service providers (CSPs), such as denial of service, shared technology vulnerabilities and CSP data loss, and system vulnerabilities are no more ranked as important for the Cloud user perspective. This suggests an increased maturity of the cloud user understanding of the cloud, on one side, but should not lower the attention on such threats from the CSP perspective. It is interesting to note that the top threats reported are more in the area of potential control plane weaknesses and limited cloud visibility. Misconfiguration and inadequate change of control, for instance, are ranked at position number two. Misconfiguration is the leading cause of data breaches in the cloud. Also, the absence of an automatic proactive change of control is perceived as another risky weakness.

Our threat taxonomy is a consolidation of threats previously considered in other documents/reports and is composed of the following groups.

- TG3.1 – Unintentional damage/loss of information or IT assets: This group includes all threats causing unintentional security leakage due to human errors.
- TG3.2 – Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties (including cloud internal communication channels). This TG, depending on the circumstances of the incident, could, also, be linked to TG3.5.
- TG3.3 – Poisoning: This group includes all the threats due to configuration/business process poisoning and aiming to alter system behaviours (i.e., at any layers).
- TG3.4 – Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure at any layers like management hijacking and identity fraud.
- TG3.5 – Legal: This group provides for threats resulting from violation of laws and/or regulations, such as the inappropriate use of Intellectual Property Rights, the misuse of personal data, the necessity to comply with judiciary decisions dictated with the rule of law. Section 4 of the present document will discuss aspects of this TG.
- TG3.6 – Organisational threats: This group includes threats to the organizational sphere.

3.5.2. New Threats and COVID-19

The enterprise cybersecurity situation got exacerbated by the emergence of COVID-19 pandemic particularly owing to the security teams' overload and distracted remote

workers.[70] Prior to the pandemic remote working was not omnipresent or even desirable for most companies. However, as the pandemic progressed, an increasing number of workers were forced to embrace this way of working. During the process, desktop virtualization solutions were rolled out in a haste, without paying attention to crucial security details including configuration hardening and endpoint protection (T3.6.5). In turn, this exposed sensitive information to potential attackers.[71] According to the survey issued by VMware Carbon Black, 89% of surveyed respondents experienced attacks by COVID-19 related malware (T3.4.8). Moreover, the number of potential targets relying on VPN has significantly increased, resulting in a substantially higher number of reported attacks. According to the aforementioned report, respondents identified remote access inefficiencies, VPN vulnerabilities and staff shortage as the main challenges in the era of COVID-19. The most targeted industries include financial, healthcare, professional services and retail, while the main motive lies in financial gains. Significant amount of attacks shows a sign of lateral movement, which is fuelled by misuse of WMI, Google Drive and process hollowing (T3.6.3). The survey carried out by Fugue on 300 IT, cloud and security professionals[72] indicates that the vast majority of cloud engineering teams that have transitioned to working from home are concerned about emerging security vulnerabilities concerning security policies, networks and devices used for managing cloud infrastructure remotely (T3.6.4). The survey also indicates that a large number of organizations experienced cloud security breach, out of which 28% were critical. Furthermore, cloud misconfiguration is one of the most widespread concerns among professionals (T3.3.1). The main reasons of cloud misconfiguration can be summarized as follows: i) lack of awareness of cloud security and policies, ii) lack of adequate controls and oversight, iii) large number of inadequately regulated APIs and interfaces, iv) careless insider behaviour.
Another concerning issue is that a significant number of cloud teams to this date still rely on slow and manual processes for maintaining cloud configuration, which leads to the impending difficulties: i) human error in missing critical misconfigurations, ii) human error while remediating critical misconfigurations, iii) difficulties in hiring new cloud security experts, iv) high cost of managing cloud misconfiguration.

Table 8 shows an update with respect to D4.1 of the cybersecurity threat map in the data domain. In particular, four threats have been added as follows.

Threat 3.4.8: Phishing – COVID-19. Amidst COVID-19 crisis, there has been a rise in the number of malicious emails based on social engineering that persuade users to provide their sensitive information. This is especially prominent in healthcare, where attackers can pose as trusted sources, such as the World Health Organization and cause damage to both individuals and organizations. Even if phishing can be considered a threat to a user it is also affected in many case systems- domain assets such as OS.

Threat 3.6.3: The lack of awareness – COVID-19. The lack of awareness and underestimation of cybersecurity threats tend to remain overlooked during the time when mitigating ever-increasing operational stress and addressing liquidity issues, health and vivacity of the work remain the priority of the most of organizations. In the cloud paradigm the shared responsibility principle allows to delegate some but not always all of the security

[70] Report Details COVID-19 Threat to Enterprise Cybersecurity https://virtualizationreview.com/articles/2020/08/07/carbon-black-report.aspx
[71] IT Security in times of the Coronavirus is both different and diverse https://sec-consult.com/en/blog/2020/03/it-security-in-times-of-corona-is-different-and-diverse/
[72] Cloud Security Risks Rise During the Coronavirus Pandemic: Survey https://cisomag.eccouncil.org/cloud-security-risks-rise-during-the-coronavirus-pandemic-survey/

aspects to the provider. During the pandemic due to the stress affecting any decisions, such delegation was in most of the cases considered as a complete delegation of responsibility opening to security issues.

Threat 3.6.4: Personal cloud service adoption – COVID-19. Remote work resulted in many communications to happen outside company firewalls, resulting in an increasing number of risks posed by malicious actors. Besides this, dependence of outsourced tools and web-based services can even further expose organizations and individuals to the risks.[73] Most of these tools are cloud based and they suffered of the rapid adoption due to the pandemic and were not capable to scale and improve security features prior to being used for their weaknesses.

Threat 3.6.5: Cloud sprawl – COVID-19. Swift adopting of cloud computing solutions within an enterprise and ignoring the way they are managed increases the possibility of remote employees creating undesired attack vector for attackers and contributing to cloud sprawl.[74] In addition, users tend to use cloud services as shadow IT even inside the company more than before, due to the need to partial work at home and the maturity of some of them was not adequate.

Table 8: Update on cybersecurity threat map in the system domain

Domain (D)	**Threat Group (TG)**	**Threats (T)**
System (3)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2)
	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (data breach) (2)
	Poisoning (3)	Configuration poisoning (1) Business process poisoning (2)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2) Malicious code/software /activity (3) Generation and use of rogue certificates (4) Misuse of assurance tools (5) Failures of business process (6) Code execution and injection (insecure APIs) (7) **Phishing – COVID-19 (8)**
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1) Malicious insider (2) **The lack of awareness – COVID-19 (3) Supply chain threats – COVID-19 (4) Cloud sprawl – COVID-19 (5)**

[73] COVID-19 CYBER SECURITY THREATS TO MSMEs https://iccwbo.org/content/uploads/sites/3/2020/05/2020-icc-sos-cybersecurity.pdf

[74] How COVID-19 is Affecting Cloud Security—and What to Do About It https://www.dsm.net/it-solutions-blog/covid-19-cloud-security

3.5.3. Gaps and Challenges

In this section, we provide an overview of gaps and challenges that impact the cybersecurity System domain, discussing those scenarios where further research and investigations are required.
Initially, we complete the analysis done in this section with those gaps and challenges that either affect the system domain alone or in conjunction with other domains. Then We provide a binding between identified threats, relevant assets and described gaps/challenges as presented in Table 9.
In a nutshell, many solutions rely on configuration hardening, which can be often neglected due to the users' lack of awareness, visibility or skills and which can in turn lead to the emergence of numerous security vulnerabilities. These vulnerabilities range from sensitive information exposure and data thefts, VPN vulnerabilities to different kinds of attacks, such as DoS attacks. On top of that, there are risks related to the use of cryptography, access control and key management, control planes, increasing complexity and exposure to the malware. As a matter of fact, system security and in particular cloud security is responsibility for both the service providers and the users. Certain responsibilities are solely providers' and solely users', while some depend on the service models. Responsibilities such as network accessibility and safeguarding, industry standards, hardware capabilities and patching are always providers. On the other hand, protection from the unauthorized access, cloud-based data protection and configuration hardening are responsibilities depending on the users. User interfaces act as entrance points to the clouds and their inadequate design can create a backdoor for attackers who can abuse the security weaknesses and cause irreversible damage to the organizations and users. Moreover, inadequate authentication to the cloud services resulting from the negligence and use of insecure storage methods can lead to the phishing attacks and ultimately loss of the credentials. When it comes to the providers, the lack of industry standards, network capabilities and hardware insufficiency can lead to the difficulties in maintaining service uptime and reliability. This can in turn open the door for DoS attacks and even further exacerbate services. Solving these issues requires additional expertise for service providers and additional training for the users and organizations. Due to the ever-growing importance and popularity of the virtualization and cloud services, as well as its correlation with the other domains, the gaps identified in this section also affect all the other domains.

System Domain-Specific Gaps and Challenges

G3.1 - Gaps on the use of cryptography. Cryptography-based security mitigations come with an additional layer of complexity, i.e. they introduce an overhead that can affect the performance and availability of the virtualized systems. Therefore, to prevent possible risks of DoS attacks, performance has to be kept under control by applying the appropriate cryptography. In the recent years, there has been an array of researches and initiatives related to cryptographic solutions going on, including the topics of Virtual Trusted Platform Module (vTPM), "cryptography-as-a-service" and post-quantum cryptography. Gaps on the

use of cryptography affect different components, such as hypervisors, guest machines, network and storage[757677].

G3.2 - Gaps on data control. The rapid advancements in communication and storage technologies have brought new challenges in the area of data privacy and protection. One of the well-known privacy problems occurs when a user provides its data to a third party and partially loses control over it. This issue is especially prevalent in cloud environments. The optimal solution to this problem is to provide verifiable and privacy-enhanced data management, which would in turn enable users to maintain a control over their data, their distribution and sharing. Another potential privacy problem is the so called "data remanence" problem, which occurs when the residual data remains on VM disk even after VM is deleted and deletion attempts are made. This issue can affect virtualization in IaaS cloud models in a way that sensitive data is unwillingly disclosed. Moreover, it can also occur after cloning and snapshotting VM, as well as, a result of malicious intentions of users foraging for sensitive data.

G3.3 - Gaps on multi tenancy, isolation and resource management. Virtualized systems are frequently based on multi-tenant systems, where multiple users share the same resources and every user is giving a dedicated share of data, configuration, functional and non-functional properties. Therefore, isolating the behaviour of different virtual machines is of the essence. As of current, there is a major gap to find a balance between complete isolation and necessity to control and monitor, with the aim of avoiding potential threats such as covert channel attacks. Another serious gap which can lead to threats such as resource hijacking and data leakage is related to the lack of adequate solutions for controlling communication between components and virtualization. Lastly, there is a need for optimizing resource management in order to respond to variable loads, as well as to increase efficiency and reduce the operational costs and probability of attacks related to the system availability and reliability.

G3.4 - Gaps on roles and human resources. There is a gap related to the need for different administration levels, especially when dealing with the virtual storage and sharing of data/resources. This gap requires balancing the protection of users' security and privacy and privileges given to virtualized environment's administrators, as well as consideration of the hierarchical system administration approach, i.e. with physical platform administrators on the bottom and multi-layered management systems on the top. Moreover, the gap involving the lack of skilled personnel responsible for deploying/configuring virtualized environments and maintaining its security also has to be filled.

G3.5 - Gaps on security assurance and Service Level Agreements (SLAs). Due to the intrinsic characteristics of virtualized and cloud systems, existing assurance techniques, such as audit, compliance and certification are rendered irrelevant. Filling this gap requires consideration of the intrinsic dynamics of virtualized systems, where multi-layer architecture consists of distributed components. Another gap caused by the multi-tenant nature of virtualization environments is related to the definition and enforcement of SLAs.

[75] Jordi Cucurull, Sandra Guasch, Virtual TPM for a secure cloud: fallacy or reality?, RECSI 2014

[76] See Peter W. Shor "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer" in https://arxiv.org/abs/quant-ph/9508027 and Bernstein "Introduction topost-quantum cryptography" in http://www.springer.com/it/book/9783540887010

[77] See https://www.trust.informatik.tu-darmstadt.de/publications/publication-%20details/?no_cache=1&tx_bibtex_pi1[pub_id]=TUD-CS-2013-0089, or Berson et al. Cryptography as a Network Service in http://www.csl.sri.com/users/ddean/papers/ndss2001b.pdf

Since virtualized environments are shared among different users their performance is greatly affected. Due to the possible interference between different SLAs there is a need to leverage the satisfaction level of the users [5]. Therefore, existing SLAs have to cope with the virtualization oddities and virtualized context, intrinsic dynamics and event-based management, as well as with the number of other related gaps, including sharing, continuous control of security and privacy conditions, SLA management and cloud security certification.

G3.6 - Gaps on forensics. Process of data analysis in virtualized environments and tasks of identification, recovery and preservation can be very complex, due to the dynamic nature of technical operations and controls and the distributed nature of data storage. Moreover, data in the cloud can be distributed across several different countries, with each having different laws. On the other hand, since the environment and resources are shared between different users, activities of the particular tenants can permanently jeopardize the evidence. Timely notifications of breaches are of the crucial essence for providing effective forensics. In addition, virtualized environment forensics require profound technical skills and the relevant support of the service providers that require forensics analysis, which is not often the case.

G3.7 - Gaps on standards/regulations. European cloud computing strategy mentions the following gaps on cloud environment services standardization: i) interoperability solutions for implementing standardized services, ii) standard certificates of communication service providers (CSPs) that enable comparison and selection of offerings, and iii) transparency in cloud SLAs.
Data formats and interfaces interoperability of cloud services epitomises a key ingredient in ensuring compatibility between independent systems. It can be achieved by standardization. Furthermore, SLAs adoption can alleviate the process of comparing the CSP cloud offerings, and thus contribute in balancing between the risks of the customer and the CSP and the lack of the appropriate SLA. Furthermore, not all cloud providers meet all required industry standards, and lack of those can result in censures and fines that can impact users/organizations. To mitigate these issues, users/organizations have to check in advance whether the desired providers meet the necessary industry standards.

G3.8 - Lack of visibility/control. One of the main advantages of a cloud system, i.e. not having to perform software, platform, and assets management on a daily basis comes at the price of having less control and visibility of the assets. It affects users/organizations in a way that it curbs their ability to verify the efficiency of their security controls, perform incident response plans and conducts data analysis related to the services and users. Users/organizations can mitigate the problem by reviewing and agreeing to the threshold concerning the amount of data they can access, the ways to track the data and security mechanisms for preventing data breaches[78].

G3.9 - Misconfiguration and inadequate change of control. Misconfiguration and inadequate change of control is one of the most prevalent challenges that cloud services are facing and its consequences can be ravaging. In 2017, private data of 123 million American households was mistakenly exposed due to the misconfiguration of AWS S3 cloud storage bucket. The data was sold to data analytics company Alteryx, which exposed the file[7980].

[78] See https://www.compuquip.com/blog/cloud-security-challenges-and-risks
[79] See https://accedere.io/pdf/Cloud%20Security%20Assessment.pdf
[80]See https://cloudsecurityalliance.org/blog/2020/02/18/cloud-security-challenges-in-2020/

G3.10 - Lack of cloud security architecture and strategy. During the migration of IT assets to clouds, organizations often disregard security architecture for repelling cyberattacks. Coupled with the lack of understanding of the shared security responsibility model, this can lead to involuntary data exposure to an array of cybersecurity threats[45].

G3.11 - Insufficient identity, credential, access and key management. Digital identity and access management are essential parts of cybersecurity which control privileged access to sensitive resources. Cloud computing brings multiple changes that profoundly impact those traits and keeping the control of identity and access management is especially of the essence with heavier use of cloud. Thus, both CSPs and cloud users are obliged to manage identity and access management while keeping attention on security. Having an identity service platform that employs robust, persistent and verified identity controls is also of great importance[45].

G3.12 - Insider threat. According to the Ponemon Institute's 2018 Cost of Insider Threats study[81], insider negligence is the main suspect of majority security incidents. Moreover, employee or contractor negligence is held responsible for 64 % of the insider accidents. The most common reasons for this threat include misconfiguration of cloud servers, phishing emails and employees storing sensitive data on the insecure devices and systems.

G3.13 - Weak control planes. Transition to the cloud requires the creation of enough data storage and appropriate protection, which in turn requires the development of new data duplication, migration and storage processes. Control plane emerges as an optimal solution for this challenge, due to the fact that it can provide necessary security and integrity in addition to the stability and data runtime. Having a vulnerable control plane can result in lack of control of data infrastructure, security and verification. As a matter of fact, controlling stakeholders can end up not knowing the security configuration, data flow patterns and weak spots, which can ultimately lead to data corruption, unavailability, and leakage[4647].

G3.14 - Abuse and nefarious use of cloud services. Malicious actors can use cloud resources for targeting users/organizations and hosting malware on cloud services. Cloud-hosted malware can seem to be genuine due to the CSP's domain, and attackers can deploy cloud-sharing tools to further infiltrate themselves[45].

G3.15 - Insecure interfaces and APIs. The security and availability of cloud services are dependent on the user interfaces and APIs, which pose as gateways to the cloud. Hence, it is crucial for those interfaces to be designed in a way that offers protection against both accidental and malicious endeavours to breach the security. Improper design of interfaces can lead to a number of critical issues, ranging from misuse to the major data breaches. Hence, users/organizations must have a thorough knowledge of the security requirements concerning the design of APIs and user interfaces[46].

G3.16 - Account hijacking due to the inadequate authentication. In the domain of cloud, cloud service accounts and subscriptions are under the highest risk of getting exploited.

[81] See https://www.illusivenetworks.com/resources/2018-ponemon-institute-research-report

There is a range of attacks that can compromise accounts security, such as phishing attacks, exploitation of cloud-based systems and stolen credentials. Similarly, due to the lack of complexity and secure storage methods in operating systems, spoofing can result in identity and data theft.

G3.17 – Vulnerabilities exposure due to increasing complexity. Operating systems contain thousands of lines of codes written and debugged by humans. Consequently, they have a significant number of involuntary introduced vulnerabilities, ranging from benign error messages all the way to potentially devastating errors which can lead to the loss of important data and reduction in productivity[82].

G3.18 – Malware exposure. Operating systems are highly susceptible to various kinds of malware, including viruses, trojans and spyware. Malware can often compromise local machines and exploit them for attacking the other systems. In order to avoid malware attacks, Rath and Kumar [6] suggest that operating systems could deploy the following mechanisms: Sandboxes, i.e. are environments in which programs can be executed without affecting the rest of the machine. Allowing limited interaction with the outside and at the same time providing the full functionality of the operating system, i.e. third-party software can be allowed minimum access to file systems.

G3.19 - Race conditions. It is of an essence to consider race conditions involving memory coherence model that take place at the time when multiple programs operate simultaneously [7] [8] [9][83]. For instance, in a situation where a privileged program that checks readability of the file and tries to open the file as root, an attacker can pass a symbolic link in the time window between two operations and then replace it with a link to the protected file. That way the attacker can get direct access to the protected file and infiltrate into the system. In other words, an attacker can take advantage of the race condition between two operations and compromise the operating system. The only workaround is enabling only atomic operations for file accessing and imposing strict restrictions on their access for all users, with the exception of the root user [6].

Gaps and Challenges in the Era of COVID-19

Emergence of COVID-19 resulted in additional gaps and challenges to the cybersecurity of systems, particularly cloud and virtualization. Moreover, the events during COVID-19 bolstered the significance of the other gaps, especially G3.8, G3.9, G3.12, G3.16 and G3.18. Misconfiguration and inadequate change of control (G3.9) and insider threat (G3.12) gained even more importance, due to the fact that negligence of the configuration hardening and endpoint protection can lead to serious vulnerabilities which would in turn allow attackers to gain the sensitive information. Hence, addressing this gap is of crucial importance. Coping with this gap during the COVID-19 era requires empowering security teams to be more proactive, establishing digital distancing practices by using separate routers for personal and work purposes and allowing real-time updates across VPN. Increased usage of cloud services has led to the significant logistic challenges for cloud service providers. In other words, greatly increased demand for cloud services, such as videoconferencing and for content providers, such as Netflix requires more human and technology resources. In addition, new gaps encompassing endpoint controls, network controls and user awareness have emerged.

[82] See https://itstillworks.com/operating-system-security-issues-6691860.html
[83] See https://www.iisec.ac.jp/proc/vol0005/hashimoto13.pdf

The following is the list of gaps and challenges during the COVID-19 era:

G3.20 – Logistic challenges to the ever-increasing cloud usage. Remote workers put previously never experienced pressure on the capacity of networks, resources and cloud systems. Moreover, the rapid rise of streaming services' usage also calls for increased bandwidth on the internet and on the cloud providers' networks. This ultimately results in the difficulties to maintain service availability and performance, as well as with shortage of required components for powering the cloud data center results.[84] Unpreparedness and inability to cope with such issues can lead to security vulnerabilities, where potential DDoS attack could even further cripple already overwhelmed systems.

G3.21 – Gaps on endpoint controls. In order to secure remote workers from potential malicious activities, organizations have to deploy multi-layer endpoint agents on all employee endpoints. Furthermore, systems should be hardened according to the proposed CIS benchmarks to prevent attackers for gaining systems' access and privileges. Default settings may not be sufficient for preventing virtual sessions from attacks

G3.22 – Gaps on Cloud user awareness. Remote workers require training on the various topics, including phishing, password guidance, privacy screen, device hardening, working with confidential materials and securing physical computing assets. In addition, security controls require continuous evaluation throughout recommended team exercises. On top of that, privileged users, such as administrators should have distinct accounts and are only able to use them on dedicated Privileged Access Workstations (PAWs) when the necessity arises.[85]

G3.23 – Gaps on remote network controls. Off-network communications from virtual desktops should be limited only to whitelisted necessary resources. Moreover, shift from full-tunnel to split-tunnel VPN could result in reducing network visibility, which can in turn be bolstered throughout the means of a cloud proxy. Any traffic occurring from the VPN has to be linked to the source IP address, while assignment of IP addresses should be linked to the corresponding user accounts. This way potential issues related to IP address identification, such as hinderance by load balancers, proxies, DNS configurations and DHCP pools can be mitigated.[85]

Cross-Cutting Gaps and Challenges

Since its inception, the use of cloud computing has significantly risen primarily owing to the higher availability of high-quality networks, low-cost computers, and increased adoption of hardware virtualization and service-oriented architecture. Cloud computing has been used in a range of business spheres, for which it provides numerous benefits such as reliable data storage. Moreover, it facilitates collaborations between employees, thus allowing for a more streamlined organization, online meetings, and completion of the projects, which in turn provides benefits for businesses.[86] However, with all of the perks that it brings, the cloud also brings the risks of cyberattacks. To avoid cybersecurity threats,

[84] When Cloud Meets COVID-19, Opportunities and Threats Emerge https://www.gartner.com/en/documents/3983341/when-cloud-meets-covid-19-opportunities-and-threats-emer

[85] Remote Work in an Age of COVID-19 — Threat Modeling the Risks https://www.fireeye.com/blog/executive-perspective/2020/03/remote-work-in-an-age-of-covid-19-threat-modeling-the-risks.html

[86] Business Benefits of Cloud Computing https://www.grouponeit.com/business-benefits-of-cloud-computing/

proper cloud configuration, and understanding of potential consequences are of the essence. That is especially the case due to the fact that the system usage, and in particular cloud and virtualization permeate other business domains, including security. As a matter of fact, when it comes to data domain sensitive data is stored on cloud services. In the human domain, the cloud allows remote collaboration of employees no matter where they are located. In addition, cloud services are used to power the IoT through the means of storing and processing IoT data and enabling management, connection and security for IoT devices. Moreover, the cloud enables support for cloud-based applications, located on remote servers and operated by third-party service providers that are used for various tasks, such as word processing, email, data collection, customer relationship management (CRM), and inventory management among many others. [87] On the other hand, the quality of virtualization and cloud services are closely correlated with the quality of the network, both providers' and users'.

Hence, the role of the systems and particularly cloud as a platform for providing various services are apparent in all of the other domains. When it comes to the identified gaps**, gaps on regulations/standards, insufficient identity, credential, access and key management** and **gaps on malware** are horizontal gaps applying to **all** domains. **Use of cryptography** also affects **data, application** and **IoT/Device**. Gaps on **network controls** and **logistic challenges to the ever-increasing cloud usage** mostly affect the networks. This is especially the case during the COVID-19 era when networks face record load owing to the considerably increased usage. **Lack of visibility/control, lack of cloud security architecture and strategy, insider threats, abuse and nefarious use of cloud services** affect user and data. Finally, **misconfiguration and inadequate change of control** and **gaps on endpoint controls** mostly apply to the **user** domain. In these cases, human behaviour, i.e. inadequate skills and carelessness are the main culprits for accomplishing security. Table 9 shows how gaps in the system domain affect the other domains of interest of CONCORDIA.

Table 9: Cross-Cutting Gaps

Gaps	**Additional Domains**
G3.1 - Gaps on the use of cryptography	Application, IoT/Device, Data
G3.2 - Gaps on data control	All
G3.3 - Gaps on multi tenancy, isolation and resource management	Data
G3.4 - Gaps on roles and human resources	User
G3.5 - Gaps on security assurance and Service Level Agreements (SLAs)	-
G3.6 - Gaps on forensics	Data
G3.7 - Gaps on regulations/standards	Data, Application
G3.8 - Lack of visibility/control	User, Data
G3.9 - Misconfiguration and inadequate change of control	User
G3.10 - Lack of cloud security architecture and strategy	User, Data
G3.11 - Insufficient identity, credential, access and key management	All
G3.12 - Insider threat	User, Data
G3.13 - Weak control planes	-
G3.14 - Abuse and nefarious use of cloud services	User, Data
G3.15 - Insecure interfaces and APIs	Application, IoT/Device
G3.16 - Account hijacking due to the inadequate authentication	All
G3.17 - Vulnerabilities exposure due to increasing complexity	Application, IoT/Device
G3.18 – Malware exposure	All
G3.19 - Race conditions	-

[87] See https://searchcloudcomputing.techtarget.com/definition/cloud-application

G3.20 - Logistic challenges to the ever-increasing cloud usage	Network
G3.21 - Gaps on endpoint controls	User
G3.22 - Gaps on Cloud user awareness	User, Network
G3.23 - Gaps on remote network controls	Network

Table 10 provides a binding between identified threats, relevant assets and gaps/challenges in this section.

Table 10: Mapping Assets, Threats and Gaps

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 G3.12 G3.22
	Inadequate design and planning or incorrect adaptation (2)	Middleware, Management, Infrastructure	G3.10
Interception and unauthorised acquisition (2)	Interception of information (1)	Network, Computer Nodes, Management Server/Console, Access Control/Authorization	G3.3 G3.19 G3.23
	Unauthorized acquisition of information (data breach) (2)	Data	G3.2 G3.3 G3.6 G3.15
Poisoning (3)	Configuration poisoning (1)	Middleware, Management, Infrastructure, Security Mechanisms	G3.18
	Business process poisoning (2)	Middleware, Management, Infrastructure, Security Mechanisms	G3.18
Nefarious activity/abuse (4)	Identity fraud (1)	Middleware, Management, Security Mechanisms	G3.3 G3.14 G3.16
	Denial of service (2)	Middleware, Infrastructure, Security Mechanisms	G3.1 G3.20
	Malicious code/software/activity (3)	Middleware, Security Mechanisms, Virtual File Format	G3.14 G3.15 G3.18
	Generation and use of rogue certificates (4)	Middleware, Management, Infrastructure, Security Mechanisms	G3.7 G3.14
	Misuse of assurance tools (5)	Data, Middleware, Management, Infrastructure, Security Mechanisms	G3.13 G3.21
	Failures of the business process (6)	Virtual machine, Platforms, Infrastructure	G3.11 G3.17
	Code execution and injection (insecure APIs) (7)	Middleware, Virtual machine, Platforms	G3.15
	Phishing (8)	Data, Middleware	G3.16
Legal (5)	Violation of laws or regulations (1)	All assets.	G3.5 G3.7
Organisational threats (6)	Skill shortage (1)	Roles	G3.4 G3.9 G3.13
	Malicious insider (2)	Data, Middleware, Management, Infrastructure, Security Mechanisms	G3.12 G3.16
	The lack of awareness (3)	Roles	G3.9 G3.10 G3.12 G3.22

	Personal cloud service adoption – COVID-19(4)	Management, Security Mechanisms, Middleware	G3.21
	Cloud sprawl (5)	Roles	G3.10 G3.22

3.6. Data-Centric Security

3.6.1. Threats (from D4.1)

In this section we provide a summary of the threat categories identified in D4.1 in the domain data. More details are reported in De 4.1. In general, threats, such as network outage or malfunctions of the supporting infrastructure, may heavily affect Big Data. In fact, since Big Data has millions of data items and each item may be stored in a separate physical location, this architecture leads to a heavier reliance on the interconnections between servers. Also, physical attacks (deliberate and intentional), natural and environmental disasters, and failures/malfunction (e.g. malfunction of the ICT supporting infrastructure), since their effects are strongly mitigated by the intrinsic redundancy of Big Data, though Big Data owners deploying their systems in private clouds or other on-premises infrastructure should take these attacks under serious consideration.

Data are compromised at huge rates, more than 25 million records compromised in the first semester of 2018,[88] with an increased cost of 6.4% in 2018. The average cost of a data breach raised to $3.9 million, while the average number of breached records by country was 25,575, with a cost per lost records of 150$ and time to identify and contain a breach 279 days.[89] In the first six months of 2019, more than 3,800 breaches have been publicly disclosed with 4.1 billion compromised records.[90] According to ENISA,[91] in 2019, we observed a 54% increase in the total number of breaches, 71% of which were financially motivated and 52% of which involved hacking. Other tactics utilized are social attacks (33%), malware (28%) and mistakes or errors (21%). In addition, the cost of data breaches to enterprises or large organizations with more than 25.000 employees is €173 per employee, with a total amount of ca. €4,33 million. The cost of data breaches for small companies with 500-1.000 employees is on average ca. €3.000 per employee, with a total amount of ca. €2,24 million for small businesses. Again, healthcare domain is a preferred target and breaches caused by system glitches or human errors have an important cost (ca. €2,74 million on average).

According to ENISA Big Data Threat Landscape,[92] a threat to a Big Data asset can be considered as *"any circumstance or event that affects, often simultaneously, big volumes of data and/or data in various sources and of various types and/or data of great value"*. It can be further divided in Big Data breach when "*a digital information asset is stolen by attackers by breaking into the ICT systems or networks where it is held/transported*" and Big Data Leak "*the (total or partial) accidental disclosure of a Big Data asset at a certain stage of its lifecycle […] due to inadequate design, improper software adaptation or when*

[88] WP2018 O.1.2.1 - ENISA Threat Landscape 2018 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/

[89] Ponemon Institute's Cost of a Data Breach Report 2019

[90] Data Breaches Expose 4.1 Billion Records In First Six Months Of 2019 https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/?sh=6313d6f2bd54

[91] ENISA Threat Landscape 2020 - Data Breach https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach

[92] WP2018 O.1.2.1 - ENISA Threat Landscape 2018 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018/

a business process fails". A Big Data Breach involves a malicious attacker behavior resulting in an unauthorised access, while a Big Data Leak involves an honest-but-curious attacker or an observer.
The threat taxonomy is a consolidation of threats previously considered in other documents/reports and is composed of the following groups.

- TG4.1 – Unintentional damage/loss of information or IT assets: This group includes all threats causing unintentional information leakage or sharing due to human errors.
- TG4.2 – Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties. This TG, depending on the circumstances of the incident, could, also, be linked to TG4.5.
- TG4.3 – Poisoning: This group includes all threats due to data/model poisoning and aims to picture a scenario that does not adhere to reality.
- TG4.4 – Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure of the victim, including the installation or use of malicious tools and software.
- TG4.5 – Legal: This group includes threats due to violation of laws or regulations, the breach of legislation, the failure to meet contractual requirements, the unauthorised use of Intellectual Property resources, the abuse of personal data, the necessity to obey judiciary decisions and court orders. We will discuss all these issues in detail in Section 4.
- TG4.6 – Organisational threats: This group includes threats to the organizational sphere.

3.6.2. New Threats and COVID-19

COVID-19 Pandemic has brought a significant increase in cyber attacks, which directly or indirectly involves threats to data. Correct and robust data management is more critical than ever, due to the fact that COVID-19 has changed our normality accelerating the distribution of computation to homes and the "periphery".[93] ENISA in its threat landscape[94] discussed how COVID-19 made cybersecurity the challenge and the opportunity in the pandemic transformation at the same time. According to EUROPOL, the new normal after COVID-19 must "*Protect your children, house, finances and data now that confinement measures are starting to relax. Criminals are still looking for victims*" [95] .Shopping, working and learning are in fact delivered online at a scale never seen before[96]. Criminals changed their behaviour to take advantages from the pandemic (showing criminal opportunism), building on the uncertainty of the scenario and the difficulties in distinguishing between reliable and unreliable information[97]. 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[98]. Lockdown first and remote working moved the computation away from businesses data centers increasing the risks of loss and interception

[93] ENISA Threat Landscape - Emerging trends https://www.enisa.europa.eu/publications/emerging-trends
[94] ENISA Threat Landscape - The year in review https://www.enisa.europa.eu/publications/year-in-review
[95] A safety guide for the 'new normal' after COVID-19 https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/safety-guide-for-new-normal-after-covid-19
[96] COVID-19 sparks upward trend in cybercrime https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime
[97] INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020, EUROPOL
[98] ENISA Threat Landscape 2020 – Ransomware https://www.enisa.europa.eu/publications/ransomware

of information, data breaches, unauthorized acquisition of information, and in general malicious attacks (T4.1.3). Data compromise becomes key to any attacks and is amplified by increasingly effective social engineering, which builds on the so-called cybercrime as a service (CaaS) where facilitators offer their knowledge on the dark web.[99] Phishing scams and malware experienced a peak during the pandemic period and adapted their activities to target users tired by the lockdown and restrictions to freedom. Attackers masqueraded their activities aiming to capture personal data by acting as providers of information about vaccines, medical supplies and hand sanitizers, portals to apply for payment of government assistance, to name but a few examples[100] [101] [102].
The problems that the businesses are experiencing are not only the protection of their customers from phishing and social engineering attacks aimed to leak and breach customer information, but also the problem of protecting those data that are exiting boundaries that are usually confined within the organizations.[103] For instance, weak videoconferencing systems may not filter out uninvited people causing conversation eavesdropping and hijacking (T4.2.3). As another example, smart working is increasing the risk of Ransomware attacks "*due to a combination of weaker controls on home IT and a higher likelihood of users clicking on COVID-19 themed ransomware lure emails given levels of anxiety*."[104] These scenario is radically changing the threat landscape due to three main aspects: i) COVID-19 pandemic as a new threat vector; ii) attack prevention and detection that can be less effective in the new communication practices introduced by COVID-19; iii) the need of security teams to manage attacks in unfamiliar conditions, and iv) the raise in importance of staff education and awareness (T4.6.1). Generally speaking, statistics show that COVID-19 had the major impact on financial and healthcare businesses[105] [106]. Remote working also had a substantial impact on attacks with an average cost of data breach increased by 137,000$ (IBM), with a peak of attacks related to COVID-19 (e.g., scams increased by 400% in March 2020 – ReedSmith, 33,000 unemployment applicants were exposed to a data security breach - NBC).

Finally, IT security budget must be redistributed to consider perimeter security, next-generation identity and access controls, remote access, automation, security training, security for trusted third parties[107], all aspects that relate to the need of protecting data and data management platforms. PwC identifies three main actions to mitigate emerging COVID-19-related risks: secure their newly implemented remote working practices; ensure

[99] INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020, EUROPOL
[100] Staying on top of changing crime patterns, COVID-19 cyber and fraud challenges. https://home.kpmg/xx/en/home/insights/2020/05/staying-on-top-of-changing-crime-patterns.html
[101] Understanding and dealing with phishing during the covid-19 pandemic https://www.enisa.europa.eu/news/enisa-news/understanding-and-dealing-with-phishing-during-the-covid-19-pandemic
[102] COVID-19's Impact on Cybersecurity, https://www2.deloitte.com/ng/en/pages/risk/articles/covid-19-impact-cybersecurity.html
[103] Key cyber risks for banks during COVID-19, Cyber and anti-fraud controls are paramount for banks during COVID-19 and beyond. https://home.kpmg/xx/en/home/insights/2020/05/key-cyber-risks-for-banks-during-covid-19.html
[104] The rise of ransomware during COVID-19, How to adapt to the new threat environment. https://home.kpmg/xx/en/home/insights/2020/05/rise-of-ransomware-during-covid-19.html
[105] COVID-19 Cybersecurity Statistics https://www.pandasecurity.com/mediacenter/news/covid-cybersecurity-statistics/
[106] Cybersecurity in the healthcare sector during COVID-19 pandemic https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic
[107] COVID-19 crisis shifts cybersecurity priorities and budgets https://www.mckinsey.com/business-functions/risk/our-insights/covid-19-crisis-shifts-cybersecurity-priorities-and-budgets

the continuity of critical security functions; counter opportunistic threats that may be looking to take advantage of the situation.[108] However, in this context according to Statistica, the economic crises is expected to cause a cut in the cybersecurity spend of 8% in 2020.[109]

Table 11 shows an update with respect to D4.1 of the cybersecurity threat map in the data domain. In particular, two threats have been added as follows.

Threat 4.1.3: Information leakage/sharing due to hostile home network – COVID-19
This threat considers an attacker exploiting the impact of COVID-19 on businesses and people to increase its revenue in terms of information leakage/sharing. In particular, it focusses on the need of people and employees to move their activities to remote and untrusted sites, which are usually weaker that their counterpart at the business side.

Threat 4.2.3: Conversation Eavesdropping/Hijacking – COVID-19
This thread considers the increased risk of conversation eavesdropping and hijacking introduced by the exponential raise of videoconferences, on one side, and the security gaps video conferencing tools carry.

Threat 4.3.3: Unreliable Data – COVID-19
The COVID-19 pandemic evidenced the problem of selectively distinguishing between reliable and unreliable information. People have been overloaded by information about pandemics, conflicting opinions by virologists, making it nearly impossible to understand the status of the crisis and making society vulnerable. On the technical side, criminals are going beyond the simple data poisoning in T4.3.1 and adapted current cybercrime to fit the *pandemic narrative*,[110] exploiting the uncertainty of the situation and making it even more critical with fake data and research experiments. This scenario is producing a substantial increase in social engineering activities, as well as in the success rate.

Table 11: Update on cybersecurity threat map in the data domain

Domain (D)	**Threat Group (TG)**	**Threats (T)**
Data (4)	Unintentional damage / loss of information or IT assets (1)	Information leakage/sharing due to human errors (1) Inadequate design and planning or incorrect adaptation (2) **Information leakage/sharing due to hostile home network – COVID-19 (3)**
	Interception and unauthorised acquisition (2)	Interception of information (1) Unauthorised acquisition of information (data breach) (2) **Conversation Eavesdropping/Hijacking – COVID-19 (3)**
	Poisoning (3)	Data poisoning (1) Model poisoning (2) Unreliable data – COVID-19 (3)
	Nefarious activity/abuse (4)	Identity fraud (1) Denial of service (2)

[108] Managing the impact of COVID-19 on cyber security, https://www.pwccn.com/en/issues/cybersecurity-and-data-privacy/covid-19-impact-mar2020.pdf
[109] Spending on cybersecurity worldwide from 2017 to 2020 (COVID-19 adjusted) (in billion U.S. dollars) https://www.statista.com/statistics/991304/worldwide-cybersecurity-spending/
[110] INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020, EUROPOL

		Malicious code/software /activity (3) Generation and use of rogue certificates (4) Misuse of assurance tools (5) Failures of business process (6) Code execution and injection (insecure APIs) (7)
	Legal (5)	Violation of laws or regulations (1)
	Organisational threats (6)	Skill shortage (1) Malicious insider (2)

3.6.3. Gaps and Challenges

In this section, we provide an overview of the gaps and challenges that impact the cybersecurity data domain, discussing those scenarios where further research and investigations are required [111].
This analysis first aims to complete the analysis done in this section with those gaps and challenges that either affect the data domain alone or in conjunction with other domains. It then provides a binding between identified threats, relevant assets and described gaps/challenges, as presented in Table 12.
In a nutshell, many solutions rely on strong cryptography, which might not be always enough, as for instance, in scenarios with limited computational capabilities or high collection rates. There are obvious risks associated with authorization privileges and access control, which are not always enough to limit those threats related to information leakage and/or sharing due to human errors. Furthermore, leaks of data are becoming customary, due to the increasing complexity of current systems (insecure APIs), mixing Cloud/Web applications, Edge computations, microservices, which are additionally affected by inadequate design/planning or improperly adaptation an improved design of computing and storage infrastructure models, while streaming data from sensors may have issues of confidentiality that cannot be mitigated by current solutions. Personal identifiable information, as well as sensitive data, are continuously collected and stored by different players. The risk of leakage or fraudulent/unauthorized use is rising even when best security practices are in place. The safety and security of humans are at the stake, requiring sound data protection solutions and privacy approaches. In this context, GDPR represents an important ground for filling in the data protection gap, though its practical application and enforcement are still debated. Recently, the widespread diffusion of artificial intelligence and machine learning introduces important risks and challenges, where unfair inferences based on untrustworthy data and poisoned models affect automatic decision processes and autonomous systems. All these breaches require, on one side, technical countermeasures, and, on the other side, the involvement of policy makers to reflect changes in current IT environments in EU laws and legislations. A skill shortage in roles such as data scientists is also affecting the entire domain. We note that, given the central role of data in today's ecosystem, the gaps in this section directly or indirectly affect the other domains of interest.

Data Domain-Specific Gaps and Challenges

G4.1 - Gaps on data protection. Threats to privacy and confidentiality of sensor data streams are among the major gaps on data protection. In this context, loss of information, interception of sensitive data and unauthorized acquisition of information are among the most important targets of an attack. As already discussed, several cases of phishing and

[111] 6 Big Data Security Issues for 2019 and Beyond https://rtslabs.com/6-big-data-security-issues-for-2019-and-beyond/

identity fraud due to traffic capture and data mining have been recorded in recent years and amplified by COVID-19. At the same time, an increase in the power of Big Data analysis supports an unprecedented ability of inferring information threatening the personal sphere of the users, facilitating an intrusion of their privacy sphere. In this context, it becomes paramount the definition of solutions filling in this protection gap, which goes beyond the application of smart cryptographic techniques, often not applicable in current distributed environments. Real time monitoring[112] [113] and assurance techniques can play an important role in this context, while their application is still limited.

While anonymization techniques have been substantially adopted in the past, they did not always prove to be effective against advanced data inference and need-to-know/need-to-share principle. Some new approaches have been recently defined such as privacy-preserving data mining [10], modifying the data to support data mining without compromising the security of sensitive information, as well as privacy-preserving machine learning [11]. Other approaches have been defined to protect data confidentiality in modern systems by applying privacy-aware analytics based on differential privacy [12] [13].

User identity falsification[114] is another problem that affects current systems, calling for advanced authentication, authorization, and access control solutions, which protects data confidentiality, on one side and user privacy, on the other side.

In this context, it is important to have streams of trustworthy data from sensors certified when possible (see G4.6). Since centralized cryptography systems are hard to implement when a large number of resource-constrained sensors are involved, Trusted Computing (TC) can become an important approach[115] [116] .

Besides the technical aspects of data protection gaps, in 2015 ENISA has conducted a privacy-oriented assessment of Big Data. [117] ENISA has identified privacy gaps and recommendations including application of privacy by design, preservation of privacy by data analytics and the need for coherent and efficient privacy policies for big data. In addition, GDPR recently filled in the gap of the management of legal aspects pertinent to Big Data system, which can be considered as a threat to the system itself. GDPR however leaves some gaps that need still to be faced such as the practical application and enforcement of its regulations, as well as all challenges including the increasing number of extortion attacks.

G4.2 - Gaps on the use of cryptography in applications and back-end services. Cryptographic techniques are often used as a countermeasure to mitigate threats (e.g., information leakage, unauthorised acquisition of information, data breach). The adoption of such techniques in a Big Data environment can be challenging mainly related to performance and scalability, protection of microdata. Cryptographic solutions are often resource demanding adding complexity and reducing the performance on the target system. Trusted Computing and TPM technologies have been developed and new paradigms such as "cryptography-as-a-service" in cloud environments have been defined [14]. The problems of crypto-algorithms including homomorphic encryption are amplified in Big

[112] https://dataconomy.com/2017/07/10-challenges-big-data-security-privacy/

[113] 9 Key Big Data Security Issues https://cybersecurity.att.com/blogs/security-essentials/9-key-big-data-security-issues

[114] Data Security Challenges https://docs.oracle.com/cd/B10501_01/network.920/a96582/overview.htm

[115] Morris, "Trusted Platform Module" In Encyclopaedia of Cryptography and Security, Springer (2011).

[116] TPM specifications can be found at http://www.trustedcomputinggroup.org/resources/tpm_main_specification, accessed December 2015.

[117] See https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/big-data-protection/at_download/fullReport

Data environments where the flexibility and complexity of a computation are endemic[118]. Research is still active in this context[119]; interested readers can find a concise study of the current state of the art in ENISA's "Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics". Key management is also an important aspect that calls for careful consideration especially in distributed scenarios like the cloud, where centralized key management is difficult to implement[120].
The same issues apply when streams of data from sensors need to be verified and certified. Integrity verification solutions do not fit the size and collection rate of Big Data and introduces gaps in the evaluation of their trustworthiness. Alternative approaches must be found such as for instance the use of TPMs (see G4.3), the evaluation of sensor behaviours (see G4.5), and the monitoring of sensor configuration (see G4.6).

G4.3 - Gaps on computing and storage models and infrastructures. Computing and storage models and infrastructures are at the core of the data domain and represent the cornerstone of Big Data computations. Lack of standard solutions and difficulties in the portability of security controls among different open-source projects (e.g., different Hadoop versions) and Big Data vendors,[121] as well as inadequate design and planning or incorrect adaptation of a Big Data platform can result in threats to managed data. In addition, the complexity of these models and infrastructures open the door to misconfigurations and human errors, which affect the security of the whole system. Gaps still exist in the monitoring and verification of the fairness of existing models and correctness of Big Data infrastructure deployment. In addition, correctness of data collections and ingestion activities is challenging and is connected to the data protection problem in G4.1. The design and deployment of a trustworthy Big Data platform can represent a source of threats if not deeply tested and verified.

G4.4 - Gaps on roles (skill shortage). The complexity of Big Data and related models/technology results in an important gap in terms of roles and skill. Data scientists, data engineers and Big Data system administrators are increasingly requested on the market. The demand for data science and analytics worker increase, while the supply of these workers is lagging behind demand[122]. Some additional data[123]: by 2020, the demand for data scientists and data analyst proliferates to 28%; 100,000 newer jobs in the data field to be created in 2020 says the European Commission; the data science talent shortage is estimated to sum up to 1.5 million by 2020 in China; the US is expected to have 2 million data science jobs vacant in 2020. This results in unprecedented risks, opening the door to information leakage/sharing due to human errors, inadequate design, planning and configuration of Big Data infrastructures, wrong decisions due to bad models.

[118] Big Data Security – Challenges and Solutions https://www.f-secure.com/en/consulting/our-thinking/big-data-security-challenges-and-solutions
[119] See for example https://www.nsf.gov/discoveries/disc_summ.jsp?cntn_id=136673,
[120] Big Data Security: Challenges and Solutions https://www.dataversity.net/big-data-security-challenges-and-solutions/
[121] Ajit Gaddam, 'Securing Your Big Data Environment', *Community event: Black Hat USA*, Las Vegas, August 2015. https://www.blackhat.com/docs/us-15/materials/us-15-Gaddam-Securing-Your-Big-Data-Environment-wp.pdf
[122] HOW THE DEMAND FOR DATA SCIENCE SKILLS IS DISRUPTING THE JOB MARKET https://www.ibm.com/downloads/cas/3RL3VXGA
[123] Data Science Jobs is Flourishing: But Data Science Professionals Are Quitting in 2020 https://medium.com/@taylor.mark110/data-science-jobs-is-flourishing-but-data-science-professionals-are-quitting-in-2020-10448cc22f79

On the other side, Big Data administrators and other privileged users manage sensitive data in their bailiwick, potentially accessing key stores and other sensitive information[124]. All the data scientist positions are unlikely to be filled in the near future, while users might not always be conscious of or, care about the legal implications of data storage – legal implications that will be very large and wide around the world.
The gaps in this paragraph reflect gaps in education, especially universities where degrees on data science have been launched only recently. Awareness, education and training are the keys to close these gaps, concerning human resources. Unfortunately, the demand of data scientists and data engineers is running at a rate that will impede this gap to be shortly filled in by these new education projects.

G4.5 - Gaps on data trustworthiness. The ability of distinguishing between correct and incorrect/fake data is paramount and a major gap in today's systems. Trustworthy data are the cornerstone for implementing safe autonomic and adaptive processes at the basis of IoT system functionality. Wrong decisions (see G4.6), such as a smoke detector not detecting smoke properly and impairing the correct functioning of a fire alarm, can result in an incalculable damage to users. Current literature [15] seems to ignore this problem and usually assumes trustworthy data, or at least that "superiority in numbers is the most important factor in the result of a combat (cit. Clausewitz)", meaning that the availability of a huge number of devices should support trustworthy decisions, also in case a not-negligible part misbehaves.
Current autonomic and adaptive systems then take a decision on data directly coming from sensors with no filtering. Trustworthy data collection and ingestion must then be implemented, rather than traditional autonomic and adaptive processes driven by untrusted/unverified data that are accepted on the basis of the provider reputation. A proper data domain should be grounded on a standard and trustworthy data collection, which is able to distinguish fake data produced by adversaries, as well as malformed data due to malfunctioning/failures. Assurance techniques have been proposed in the past for trustworthiness evaluation; however, they target the behaviour of the system, as a whole and assume the data over which the evaluation is built to be trustworthy. The extension of assurance verification to data collection and ingestion would contribute to fill in this gap.
This gap also includes the challenge of detecting adversarial AI for the future of cyber defence systems.[125]

G4.6 - Gaps on decision support systems. Autonomic and adaptive systems are at the basis of modern systems and processes (e.g., cloud and IoT environments). Decisions are taken based on data collected on the field and involve humans as just another component of the system, with all risks and unpredictability introduced when human decisions are put in the automation loop.
Traditional autonomic and adaptive processes aim to maximize the quality of a decision (e.g., scalability), but are often driven by untrusted/unverified data that are accepted on the basis of the provider reputation. As a consequence, it is often difficult to prove/audit the correctness of such decisions, and wrong decisions can result in catastrophic events. This problem points to the need of an accountable trustworthy data collection. Solutions based on remote attestation [16] [17] or assurance [18] [19] have been provided, but still suffer from data trustworthiness challenge G4.5.

[124] Vormetric report, Trends and Future Directions in Data Security, CLOUD AND BIG DATA EDITION, 2015. See http://enterprise-encryption.vormetric.com/rs/vormetric/images/Cloud-and-BigData-Edition-2015-Vormetric-Insider-Threat-Report-Final.pdf, accessed December 2015.
[125] ENISA Threat Landscape - Emerging trends https://www.enisa.europa.eu/publications/emerging-trends

Reduction of false positives is also a long-waited promise of cybersecurity industry in its attempt to manage false alarms.[126]

G4.7 - Gaps on ethics. Data analytics, machine learning, artificial intelligence are digital technologies that will shape the future and entire humanity. A proper, fair and ethical adoption of such technologies becomes fundamental to guarantee human rights. These technologies "*have raised fundamental questions about what we should do with these systems, what the systems themselves should do, what risks they involve, and how we can control these*". The main debates concern surveillance, manipulation of behaviour, opacity of AI systems, bias in decision systems, human-robot interaction, artificial moral agents, and all resembles the concept of ethics in AI, ML, and in general data management. In this context, bias in decision systems assume an important role, connected to gap G4.6, "*when unfair judgments are made because the individual making the judgment is influenced by a characteristic that is actually irrelevant to the matter at hand, typically a discriminatory preconception about members of a group*".[127] Fairness vs. bias in machine learning and artificial intelligence is an important gap [20].[128]
Also, the European Commission has proposed guidelines on this issue with its documents[129] [130]discussing ethical rules that are suggested in the design, development, deployment, implementation or use of AI products and services in the EU and ethics guidelines for trustworthy AI. The document "The ethics of artificial intelligence: Issues and initiatives"[131] then dealt with the ethical implications and moral questions that arise from the development and implementation of artificial intelligence (AI) technologies. The document presents gaps around the mechanisms of fair benefit-sharing; assigning of responsibility; exploitation of workers; energy demands in the context of environmental and climate changes; and more complex and less certain implications of AI, such as those regarding human relationships. It considers the impact of AI on human psychology, inequality and bias, democracy, accountability and trust.

Gaps and Challenges in the Era of COVID-19
Complementary to the section regarding the impact of COVID-19 on cybersecurity threats, COVID-19 also impacts on the gaps and challenges, changing their prioritization on one side and adding some more gaps and challenges on the other side. Regarding the prioritization of gaps and challenges, the advent of COVID-19 gave a boost to gaps G4.1, G4.5, and G4.6. Data privacy and confidentiality (G4.1) become even more critical than before; remote working as well as digital interactions increased the amount of shared/collected data, strengthened requirements on secure data management and posed critical challenges introduced by the extension of IT boundaries to private houses. In this context, the introduction of hostile home networks in the picture requires careful management of data collection and verification procedures aiming to guarantee trustworthy data. The change in user and customer behaviours introduces a gap and a need for new approaches to behavioural-based evaluation of data trustworthiness. Moreover, COVID-19 introduces an important gap on the ethics of data collection, usage and management, which

[126] ENISA Threat Landscape - Emerging trends https://www.enisa.europa.eu/publications/emerging-trends
[127] Ethics of Artificial Intelligence and Robotics https://plato.stanford.edu/entries/ethics-ai/
[128] https://www.nature.com/articles/d41586-020-00160-y
[129] Ethics guidelines for trustworthy AI https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
[130] EU guidelines on ethics in artificial intelligence: Context and implementation https://www.europarl.europa.eu/RegData/etudes/BRIE/2019/640163/EPRS_BRI(2019)640163_EN.pdf
[131] The ethics of artificial intelligence: Issues and initiatives https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634452/EPRS_STU(2020)634452_EN.pdf

is caused by a new scenario mixing the different spheres of each one life, such as, private sphere, public sphere and working sphere. These public and working spheres until a few months ago (end of 2019) were clearly separated and often isolated, are mixed in a single space due to the collocation of the different users' activities.
Regarding gaps and challenges, one additional emerges due to COVID-19 as follows.

G4.8 - Gaps on video conferencing tools. The advent of COVID-19 has revolutionized the way in which meetings are held. Physical meetings are replaced by virtual meetings hosted by video conferencing tools. These tools are often unable to address the increasing demand in resources, are struggling in achieving the required scalability and most importantly have not been designed to support strong requirements on security and identity management. The risk of unauthorized participants is therefore raising.

G4.9 - Gaps on data management across borders. The advent of COVID-19 has radically changed the IT shape, changing forever the boundaries of IT systems and data centers. Users and customers are increasingly connecting to a private network from hostile sites, which were forbidden pre-COVID-19. New approaches must be devised in order to better manage remote accesses, minimizing the risks of propagating attacks such as malware and ransomware that aims to reduce availability and integrity of data.

Cross-Cutting Gaps and Challenges

Today distributed systems and services are built around data and knowledge. An unprecedented amount of data is collected every day with an increasing trend over time, making data management at the center of both research and development activities and a fundamental aspect in the cybersecurity domain. Data, in fact, are an invaluable weapon in the hands of cybersecurity defenders and an invaluable asset target of many cybersecurity attacks. Data represent the engine of transformation of the digital economy[132] and its correct management can represent a booster in any market. Data affects any (business) domain and security is not an exception. For instance, in IoT/Device domain, smart data are collected as continuous streams from smart devices; in network domain, data are fundamental for managing and adapting model software defined networks, while 5G is bringing data collection to another level; in the system domain, heterogeneous data are collected and used to support autonomous systems in optimizing their behaviour; in application domain, data are on the basis of developed applications; in human domain, data model the human knowledge and represent the most sensitive asset.
In this scenario, it clearly emerges that the fundamental role data has in each of the domains of interest both as a source of information for better protecting assets, and as an asset itself. Coming to the gaps identified in this section, **data protection** is a horizontal gap that impacts **all** domains of interest. In particular, data protection at the system/edge/IoT arises as new risks and problems which are introduced due to the widespread diffusion of resource-constrained devices, to their heterogeneity, and to the fact that they are managed by untrustworthy providers. **Use of cryptography** is a gap that mainly impacts **systems** in general and **application** and **IoT/Device** in particular, where confidentiality of data arises in its full power and cryptography struggles to keep up. **Computing and storage models and infrastructures** introduce gaps that also affect the **system** and **network** where such models are executed, and infrastructures integrated. **Data trustworthiness** and **decision support systems** is another horizontal gap that impact **all** domains of interest. In particular,

[132] DATA DRIVEN ECONOMY Market Trends and Policy Perspective http://www.itmedia-consulting.com/DOCUMENTI/datadrivensummary.pdf

data and model poisoning introduce new risks and gaps that affect modern systems and architectures, where the massive adoption of sensors pave the way to attacks where fake data are produced to either implement wrong decisions, poisoning training activities to produce models that represent wrong behaviours or cover malicious activities from an attacker. Finally, **ethics** introduce gaps that mainly affect human beings (**user**) putting their personal sphere at risk or providing an unfair environment, and the way their devices are directly or indirectly used (**IoT/Device**). Table 12 shows how gaps in the data domain affect the other domains of interest of CONCORDIA.

Table 12: Cross-Cutting Gaps

Gaps	**Additional Domains**
G4.1 - Gaps on data protection	All
G4.2 - Gaps on the use of cryptography in applications and back-end services	Application, IoT/Device, System
G4.3 - Gaps on computing and storage models and infrastructures	System, Network
G4.4 - Gaps on roles (skill shortage)	-
G4.5 - Gaps on data trustworthiness	All
G4.6 - Gaps on decision support systems	All
G4.7 - Gaps on ethics	User, IoT/Device
G4.8 - Gaps on video conferencing tools	Application, User
G4.9 - Gaps on data management across borders	All

Table 13 provides a binding between identified threats, relevant assets and gaps/challenges in this section.

Table 13: Mapping Assets, Threats and Gaps

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 G4.4 G4.8 G4.9
	Inadequate design and planning or incorrect adaptation (2)	Data, Big Data analytics, Software, Computing Infrastructure models, Storage Infrastructure models	G4.1 G4.2 G4.3 G4.4
Interception and unauthorised acquisition (2)	Interception of information (1)	Data, Roles, Infrastructure	G4.1 G4.2 G4.3 G4.4 G4.9
	Unauthorised acquisition of information (data breach) (2)	Data, Roles, Infrastructure	G4.1 G4.2 G4.3 G4.4 G4.8 G4.9
Poisoning (3)	Data poisoning (1)	Data, Security and privacy techniques, Data management, Data privacy.	G4.1 G4.4 G4.5 G4.6
	Model poisoning (2)	Data, Data Analytics	G4.1 G4.4 G4.5

			G4.6
Nefarious activity/abuse (4)	Identity fraud (1)	Data, Infrastructure	G4.1 G4.5 G4.7 G4.9
	Denial of service (2)	Infrastructure	G4.1 G4.2 G4.3
	Malicious code/software /activity (3)	Data, Software, Computing infrastructure models	G4.1 G4.2 G4.3 G4.9
	Generation and use of rogue certificates (4)	Data, Big Data analytics, Software, Hardware	G4.1 G4.2
	Misuse of assurance tools (5)	Security and Privacy Techniques, Data, Infrastructure	G4.1 G4.5 G4.6
	Failures of business process (6)	Data, Big Data analytics	G4.1 G4.4 G4.6
	Code execution and injection (insecure APIs) (7)	Data, Storage Infrastructure models	G4.1 G4.2 G4.3 G4.9
Legal (5)	Violation of laws or regulations (1)	All assets.	G4.1 G4.7
Organisational threats (6)	Skill shortage (1)	Roles	G4.1 G4.4
	Malicious insider (2)	Roles, Data, Infrastructure Security, Integrity and Reactive Security	G4.1 G4.4 G4.7

3.7. Application-Centric Security

3.7.1. Threats (from D4.1)

In this section we provide a summary of the threat categories identified in D4.1 in domain application. In general, threats, such as injection and application malfunctioning, may strongly affect IT in general. In fact, current IT systems are heavily based on applications/services composed at run time and therefore exposed to attacks and breaches. Also, attacks to hosting platforms (deliberate and intentional), failures/malfunctions (e.g. malfunction of the ICT supporting platform) can be important sources of risk. Modern applications are distributed and composed of different parts, often exposing a standard API interface (e.g., REST, RPC, etc) and interacting on virtual networks or on an orchestration platform. Such a complexity brings new threats and challenges that developers have to cope with. At the same time, "traditional" (i.e., desktop, client-side) applications suffer from long-standing issues that still today are a source of bugs and attacks. Even well-known threats such as phishing and attacks such as DoS are increasingly sophisticated.[133]

A threat to application assets can be considered as *"any circumstance or event that affects, often simultaneously, services and applications distributed over the Web"*. The threat

[133] ENISA, "ENISA Threat Landscape - Distributed Denial of Service (from January 2019 to April 2020)". https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-distributed-denial-of-service

taxonomy is a consolidation of threats previously considered in other documents/reports[134] [135]and is composed of the following groups.

- TG5.1 – Unintentional damage: This group includes all threats causing application malfunctioning or loss of confidentiality/integrity/availability, due to human errors.
- TG5.2 – Interception and unauthorised acquisition: This group includes threats introduced by alteration/manipulation of the communications between two parties. This TG, depending on the circumstances of the incident, could, also, be linked to TG5.4.
- TG5.3 – Nefarious activity/abuse: This group includes threats coming from nefarious activities. It requires active attacks targeting the platform of the victim, as well as public interfaces of the hosting platform and applications.
- TG5.4 – Legal: This group provides for threats resulting from violations of laws and/or regulations, such as the inappropriate use of Intellectual Property Rights, the misuse of personal data, the necessity to comply with judiciary decisions dictated with the rule of law. Section 4 of the present document will discuss certain aspects of this TG identified.
- TG5.5 – Organisational threats: This group includes threats to the organizational sphere.

3.7.2. New Threats and COVID-19

During the COVID-19 Pandemic the cyberthreat landscape has seen the exacerbation of existing threats exploiting the uncertainty characterizing the Pandemic, often driven by cybercrime actors. In fact, the Internet Organized Crime Threat Assessment (IOCTA 2020)[136], developed by Europol during the Pandemic times, outlined the ever-increasing usage of ransomware, phishing and scamming. These threats, in particular the last two, go beyond a mere technical aspect, demanding strong awareness on the users' side.
One notable attack exploiting scamming, which has gained also wide coverage on the media, has been the "Twitter Bitcoin Scam" of July 2020, where several Twitter accounts of famous people, including, among the others, Barack Obama and Elon Musk, have been compromised. These accounts were posting messages pointing to a bitcoin donation campaign related to the COVID-19 Pandemic. It has been then discovered that the compromise has been performed by the means of social engineering against Twitter employees[137].
Another significant incident happened in Germany in September and is believed to be the first ransomware attack against a hospital causing a death. The hospital, due to a ransomware infection, could not handle a patient which has been carried to another hospital,

[134] OWASP Top 10 -2017 The Ten Most Critical Web Application Security Risks https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf
[135] CWE/SANS TOP 25 Most Dangerous Software Errors https://www.sans.org/top25-software-errors#__utma=32063036.1074415474.1568715260.1568715260.1568715260.1&__utmb=32063036.10.9.1568715627949&__utmc=32063036&__utmx=-&__utmz=32063036.1568715260.1.1.utmcsr=google|utmccn=(organic)|utmcmd=organic|utmctr=(not%20provided)&__utmv=-&__utmk=42405799
[136] Europol, "Internet Organised Crime Threat Assessment 2020 (IOCTA)". https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf
[137] Wired, "How Twitter Survived Its Biggest Hack - and Plans to Stop the Next One". https://www.wired.com/story/inside-twitter-hack-election-plan/

causing a delay of about one hour, resulting in the death of the patient.[138] More importantly, it appears that attackers have exploited a known vulnerability, that is, a vulnerability for which an advisory and the respective fix already existed.
Also, many contact-tracing apps have been developed aiming to help healthcare systems in tracing (potential) infected people. Many of these apps have faced harsh critics, that were, in the case of decentralized approaches, mostly unjustified. For instance, Italian app Immuni,[139] which is regarded as one of the best contact-tracing apps in the EU, has been boycotted by some healthcare agencies because local managers believe it was useless. Another crucial aspect is interoperability between systems, for instance of apps of different countries[140]. As of October 2020, interoperability works only among German, Irish and Italian contact-tracing apps.
Interoperability between systems is, in fact, of paramount importance in a society that is becoming more and more digital-oriented. It is an aspect affecting also the cases of upgrading systems and integrating existing (legacy) systems with more modern ones. For instance, some US states have faced challenges in handling unemployment claims due to the Pandemic, mostly because they rely on legacy COBOL-based systems, requiring very specialized skills[141].
Finally, the lockdown imposed to fight the Pandemic has shifted many activities from in-person to remote. Videoconferencing and remote collaboration software, such as Microsoft Teams, Skype or Zoom, have seen an unprecedented spike of usage, not without concerns. On one side, these tools have shown weak communication protection, eventually leading to "organized attacks", on the other side they can significantly stress the network, to due a high bandwidth demand[142].

Table 14 shows an update with respect to D4.1 of the cybersecurity threat map in the application domain. In particular, 4 threats have been added as follows.

Threat T5.1.2: Inadequate design – COVID-19
Design is a fundamental step in every application development process, having a great impact on the final outcome. Design should take into account all the functional aspects of the application, as well as non-functional aspects such as scalability, user experience. Furthermore, design *must* take into account security aspects from the beginning, by thoroughly evaluating all the threats the application will be subjected to, and subsequently implement the proper mitigation. Compliance with existing regulations must be considered from the beginning, since they often require specific activities and guarantees to be offered. If the design phase does not consider all these factors properly, the resulting application will be weak, opening for many of the threats listed below, including possible law violations. This threat is related to *Threat T4.1.2*, in Data-Centric Security (Section 3.6.3).

[138] Ars Technica, "Patient dies after ransomware attack reroutes her to remote hospital". https://arstechnica.com/information-technology/2020/09/patient-dies-after-ransomware-attack-reroutes-her-to-remote-hospital/
[139] https://www.immuni.italia.it/en
[140] Corriere del Veneto, "Immuni, mai caricati dalle Usl i dati dei positivi in Veneto" (in Italian). https://corrieredelveneto.corriere.it/veneto/politica/20_ottobre_14/immuni-mai-caricati-usl-dati-positivi-veneto-1972382a-0dea-11eb-a0fa-5985683fd478.shtml
[141] CNN, "Wanted urgently: People who know a half century-hold computer language so states can process unemployment claims". https://edition.cnn.com/2020/04/08/business/coronavirus-cobol-programmers-new-jersey-trnd/index.html
[142] New York Times, "'Zoombombing' Becomes a Dangerous Organized Effort". https://www.nytimes.com/2020/04/03/technology/zoom-harassment-abuse-racism-fbi-warning.html

Threat T5.3.6: Supply-Chain Security – COVID-19

Supply-Chain Security refers to the security of all the components (e.g., hardware, third party software) involved in the realization of a software application or, more generically, of an ICT product.[9] [10] In fact, in case one of such components be insecure, or even infected by a malware, the final outcome will be compromised as well. This aspect is exacerbated by the complexity of existing systems.[143] Supply-chain security is connected with the concept of *trust*, since at a certain point there is no alternative than trusting a certain subject whose products are being bought. This threat encompasses several aspects, in particular hardware security, application installation and update. Hardware security refers to hardware defects, which are extremely difficult to fix in software, and can even be intentional. Application installation and update refer to all the activities involved in installing and updating an application. Threats can come from, among the others, *i)* fake applications miming the real applications users want to install, *ii)* vulnerabilities in the installation/update process (e.g., bypassing code signing or servers compromise), *iii)* vulnerabilities in third parties' software the application being installed/updated depends on. This threat can result in application tampering, malware installation, or in backdoors on users' devices. Furthermore, supply-chain attacks do not target only the final consumer, but can impact on critical infrastructures, such as power grids.[144]

Threat T5.5.2: Skill shortage – COVID-19

Systems are becoming increasingly distributed and complex and threats are constantly evolving. As such, they demand new expertise, both for developing and managing these systems and for keeping them secure and safe from novel and sophisticated threats. Skills and education are required also for other people engaging with systems, e.g., employees. This threat is related to Threat T4.6.1 in Data-Centric Security and is also related to most of the threats highlighted in this Section.

Table 14: Update on cybersecurity threat map in the application domain

Domain (D)	**Threat Group (TG)**	**Threats (T)**
Application (5)	Unintentional damage (1)	Security misconfiguration (1) **Inadequate design – COVID-19 (2)**
	Interception and unauthorised acquisition (2)	Interception of information (1) Sensitive data exposure (2)
	Nefarious activity/abuse (3)	Broken authentication and access control (1) Code execution and injection (insecure APIs) (2) Denial of service (3) Insufficient logging and monitoring (4) Untrusted composition (5) **Supply-chain security – COVID-19 (6)**
	Legal (4)	Violation of laws or regulations (1)
	Organisational threats (5)	Malicious insider (1) **Skill shortage – COVID-19 (2)**

[143] BitSight, "FBI alerts companies of Cyber Attacks Aimed at Supply Chains". https://www.bitsight.com/blog/fbi-alerts-companies-of-cyber-attacks-supply-chains

[144] Trey Herr, June Lee, William Loomis, and Stewart Scott, "Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain", 2020, https://www.atlanticcouncil.org/wp-content/uploads/2020/07/Breaking-trust-Shades-of-crisis-across-an-insecure-software-supply-chain.pdf

3.7.3. Gaps and Challenges

In this section, we provide an overview of gaps and challenges that impact the cybersecurity application domain, discussing those scenarios where further research and investigations are required.
This analysis first aims to complete the analysis done in this section with those gaps and challenges that either affect the data domain alone or in conjunction with other domains. Then it provides a binding between identified threats, relevant assets and described gaps/challenges as presented in Table 15.
In a nutshell, applications are developed as backend services whose functionalities are delivered by the means of remote APIs, for instance, web services, REST. Instead of developing monolithic applications (i.e., big applications consisting of a single code base), developers tend to *miniaturize* them by creating the so-called microservices (i.e., many small applications with independent code bases). This style of development, however, poses new challenges for applications developers and maintainers. In particular, applications are more distributed spanning, possibly, across different cloud providers and across different layers (cloud and edge). Furthermore, the orchestration of such distributed systems is increasingly complex, demanding for skilled maintainers dealing with continuous updates of (subset of) the systems. This distribution layer introduces more issues: the orchestration layer must be properly configured and secured, as well as the communication among the microservices.
Finally, these applications are delivered to end users by a web interface, therefore there is a strong focus towards providing a secure and sandboxed execution platform and browsers are constantly evolving adding security and privacy features.
These new challenges, however, are still paired with existing ones: for instance, web applications are *still* vulnerable to web-related threats, such as injections and cross-site scripting.
At the same time, operating systems and traditional desktop applications still suffer from old and well-known vulnerabilities (e.g., buffer overflows) due to implementation fault, mostly related to the programming language being used. These vulnerabilities can result in disastrous situations causing the compromise, or even the complete loss, of the data stored within a computing device.
In general, solutions aimed to improve the state of security of the aforementioned aspects do exist, but they are not applied/not applied correctly.

Application Domain-Specific Gaps and Challenges

G5.1 - Gaps on microservices-aware security. Microservices and, more in general, distributed systems, follow an established pattern for communication, which mostly happens on the HTTP protocol. Traditional network security has been implemented by the means of firewalls. However, standard firewalls fall short when considering such new systems, characterized by a dynamic topology, that is, microservices can be easily scaled horizontally or replaced by new versions, making it difficult to implement address- and port-based security rules. Some solutions offering microservice-aware network security are emerging, for instance,[145], but they are often bound to a specific platform. In fact, there is an increase in web application attacks, and, also, more companies are adopting WAF (Web Application Firewall).[146]

[145] Cilium, https://cilium.io/
[146] ENISA, "ENISA Threat Landscape - Web Application Attacks (from January 2019 to April 2020)". https://www.enisa.europa.eu/publications/web-application-attacks

G5.2 - Gaps on authentication and authorization. Microservices and API services' security needs embrace far more concepts than network security. One of the key aspects is related to authentication and authorization. They are not new issues, but the heterogeneity and the complexity of microservice-based deployment pose new challenges. [147] Microservices enable writing *polyglot* applications (i.e., different programming languages, different frameworks), and this means that developers are faced with different ways of managing authentication and authorization, eventually resulting in incoherence or vulnerabilities, especially when implementing complex access policies. Furthermore, some frameworks are extremely minimal, providing only the basic tools for authentication and authorization. At the same time, this issue is faced by client applications, often relying on password-based authentication, where users are tasked with selecting a strong password.

G5.3 - Gaps on orchestration and composition. Applications composed of hundreds or even thousands of small components need a centralized solution to manage their deployment. Managing security in such an environment is particularly difficult, because it involves securing *i)* microservices themselves (Gap G5.1), *ii)* external software being used (e.g., databases, message brokers), *iii)* the orchestration platform, the latter often perceived as complex frameworks, requiring mastering many concepts to configure a proper deployment.[148]
Finally, some architectures, despite being distributed, still have single points of failure (e.g., the so-called API gateway).[149] This fact is even exacerbated by CI/CD methodologies, where software is deployed automatically, therefore requiring proper countermeasures to avoid delivering applications with bugs or security issues (see Gap 5.6).

G5.4 - Gaps on safety and security by default. Traditional desktop applications, and in particular, operating systems are written in low-level programming languages and this often results in security vulnerabilities (memory bugs) allowing an attacker to, for instance, execute arbitrary code on the victim's device, or to gain access to victim's data, to name but a few. For instance, Microsoft Research estimates that approximately 70% of the reported vulnerabilities in Microsoft's software are caused by memory bugs. [150] This type of vulnerability is, in fact, not new, but such a statement claims for a paradigm shift towards safer development practices, delivering products which are *safe by design*. Memory-safe programming languages have been traditionally considered a poor fit for performance critical software, such as an operating system; therefore faster, but less safe, languages have been preferred. However, a change is beginning to happen, and many vendors are considering adopting safer languages, for instance, Rust[151]. Within this context, there are still gaps to fill in. In particular, while these languages are in practice, *safer*, the extent of such a claim has not been completely understood yet [21]. Furthermore, it is clearly infeasible to rewrite a whole code base from scratch; automatic translation tools producing high-quality code should be preferred instead, eventually rewriting only the most critical parts of the software, that is, modules dealing with inputs.[152] Also, to develop a new class

[147] ENISA, "ENISA Threat Landscape - Web Application Attacks (from January 2019 to April 2020)". https://www.enisa.europa.eu/publications/web-application-attacks
[148] Kubernetes, a popular container orchestration platform, has been affected by some serious vulnerabilities, for instance: https://nvd.nist.gov/vuln/detail/CVE-2019-1002101, https://nvd.nist.gov/vuln/detail/CVE-2019-112533.
[149] Jack Mannino, "Security in a Microservice World". https://owasp.org/www-pdf-archive/Microservice_Security.pdf
[150] Matt Millar "Trends, Challenges and Strategic Shifts in the Software Vulnerability Mitigation Landscape", BlueHat Israel, 2019.
[151] Rust. A language empowering everyone to build reliable and efficient software. https://www.rust-lang.org/
[152] Per Larsen, "C2Rust: Migrating Legacy Code to Rus", RustConf 2018. https://c2rust.com/

of safe-by-design products, the use of such safe languages should be encouraged and taught at different levels, from academia to industry. Next, there exists techniques aiming to improve safety of intrinsically unsafe languages, such as static and dynamic analysis, for instance, *libFuzzer.*[153] However, these tools are often separated from the main toolchains, requiring additional steps to be properly used, and manual corrections upon any errors.
Finally, the need for stronger applications featuring security and safety by default is even more critical when taking IoT devices into account.

G5.5 - Gaps on the proper management of configurations. One of the most challenging aspects of modern distributed systems development and deployment is related to the management of configuration, where often a distributed configuration store is employed. In particular, credential management is critical from the security point of view. Best practices suggest using some form of encrypted storage systems; however, they are notoriously difficult to use, or at least require some degree of expertise. In practice, recent breaches, such as [154], show that *i)* configuration stores are not secure by themselves or are not properly secured and *ii)* credentials saved within the configuration store are *still* insecure (i.e., guessable passwords). This claims for stronger and reliable ways of credentials management, which are secure by default without requiring any manual intervention. This gap is relevant also outside of the APIs environment, for instance poor credential management, (e.g., the use of default passwords, eventually difficult to change) has been always the means to compromise gateways, and then IoT devices. Also, the same applies to client-side configuration and credential storage.

G5.6 - Gaps on supply-chain security. The security and the safety of an ICT product passes from the security of all the components the ICT product builds on. In practice, supply-chain security means that the security of an application is not (completely) under the control of the developers. In the era of CPU vulnerabilities (i.e., Meltdown), of fake apps on mobile app stores and of state-sponsored attacks, supply-chain security is an important gap to fill in, as acknowledged by ENISA.[155]

G5.7 - Gaps on skills. Managing security in a landscape composed of small services whose deployment changes at a high rate is a challenging and difficult task, requiring expertise in several fields and ability to operate at the different layers of the overall application is made up of (e.g., application layer, orchestration layer). Nowadays the trend is to shift security "to the left", that is incorporating security as soon as possible in the development process, towards the so-called DevOps methodologies, permitting to catch bugs and potential security issues earlier [22]. However, these methodologies require building a "security culture"[156] among the members of the development team and requires the team to apply security in novel contexts, for instance implementing a secure deployment pipeline [23]. In turn, all these activities require knowledge beyond *traditional* cybersecurity skills, in particular the ability to *apply* and *use* existing security techniques.

[153] LLVM libFuzzer. https://llvm.org/docs/LibFuzzer.html
[154] Ars Technica. "Thousands of servers found leaking 750MB worth of passwords and keys", "https://arstechnica.com/information-technology/2018/03/thousands-of-servers-found-leaking-750-mb-worth-of-passwords-and-keys/
[155] ENISA, "ENISA Threat Landscape - Emerging Trends (from January 2019 to April 2020)". https://www.enisa.europa.eu/publications/emerging-trends
[156] Cloud Security Alliance (CSA), "The Six Pillars of DevSecOps: Collective Responsibility". https://cloudsecurityalliance.org/artifacts/devsecops-collective-responsibility/

Gaps and Challenges in the Era of COVID-19

The discussion on how COVID-19 impacted on cybersecurity threats outlined the existence of several gaps, which are detailed in the following. These gaps are not new, yet they have been exacerbated by the current situation.

G5.8 - Gaps on interoperability. Interoperability refers to the ability of different, heterogenous systems to interoperate one to each other, delivering better functionalities. COVD-19 showed an urgent need for systems interoperability, especially the ones delivering public services (e.g., healthcare). Interoperability also calls for a strong revision of existing public systems, which are often legacy and, as such, difficult to integrate with more modern systems (e.g., apps). Also, being European *Union*, interoperability of systems across national borders, is of great importance. In any case, education plays a crucial role to allow more people to take advantage of such digital services.

G5.9 - Gaps on education. Coming from gaps G5.7 and gaps G5.8, another important gap is related to education. Whereas skill (G5.7) refers to the need of skilled people dealing with cybersecurity, education refers to the need of educating *everyone* to a correct and safe use of digital technologies. In particular, users should be more aware of emerging sophisticated attacks (e.g., Twitter bitcoin scam), which rely on social engineering and phishing. This gap is related to Section 3.6 "User-centric Security". In fact, according to the "Special Eurobarometer 499"[157] users' awareness is increasing, but attacks are becoming more complex and personalised, making it more difficult to recognise and react to them.

G5.10 - Gaps on sophisticated protection. The new, sophisticated and personalised threats are pushing the boundaries of cybersecurity protection. In fact, ENISA predicts that the attack surface is continuously expanding and targeted by attacks with long-term objectives. Furthermore, remote and smart working makes it challenging to define trust boundaries and "zero-trust" is one of the proposed approaches. Finally, AI is gaining more and more attackers' attention. Together, they strongly demand for new and sophisticated forms of protections, dealing also with soft attacks exploiting the human factor, often considered the "weakest link"[158] [i]

Cross-Cutting Gaps and Challenges

Miniaturization and modern distributed systems architecture enable for a more elastic way of computing, where services can be scaled up and down more easily, allowing to quickly adapt to demands. Such flexibility requires the use of orchestration platforms and comes at the price of a **higher complexity**.

Applications are, in fact, the basis for data elaboration, IoT, networks, therefore application-centric security is a horizontal gap affecting all domains of interest. The aforementioned threats and gaps show that, in many cases, **solutions do exist**, but they are not used or **not applied correctly**. On one side, application security suffers from **long-standing issues**, due to intrinsically unsafe/insecure development processes and tools, even if safer solutions could have been used. Also, this fact is exacerbated by the advent of **IoT devices**, which makes it even more urgent to solve this problem once and for all. On the other side, backend applications are extremely complex, introducing new challenges developers have to cope

[157] Special Eurobarometer 499: Europeans' attitude towards cybersecurity". January 29, 2020. https://data.europa.eu/euodp/en/data/dataset/S2249_92_2_499_ENG

[158] ENISA. "ENISA Threat Landscape - The Year in Review (From January 2019 to April 2020). https://www.enisa.europa.eu/publications/year-in-review/at_download/fullReport

with, such as **authorization and configuration**, whose incorrect use can lead to severe issues. In fact, the development, deployment and maintenance of modern distributed systems require skilled people with wide knowledge, able to **introduce security *during* the application development process**.
Furthermore, **compliance** is a fundamental requirement, demanding strong and evincible actions. In turn, being compliant to laws and regulations requires other knowledge beyond software development and security. To conclude, **education** is a key factor towards improving application security.
Finally, **supply-chain security** models security of all the components involved in the realization of an ICT product, showing that threats come from many different places and dimensions. As such, having control on all of them is virtually impossible, but still the situation needs to be improved.
Table 15 shows how gaps in the application domain affect the other domains of interest of CONCORDIA.

Table 15: Cross-Cutting Gaps

Gaps	**Additional Domains**
G5.1 - Gaps on microservices-aware security	Data, System
G5.2 - Gaps on authentication and authorization	Data
G5.3 - Gaps on orchestration and composition	Data, System
G5.4 - Gaps on safety and security by default	All
G5.5 - Gaps on the proper management of configurations	All
G5.6 - Gaps on supply-chain security	All
G5.7 - Gaps on skills	-
G5.8 - Gaps on interoperability	All
G5.9 - Gaps on education	-
G5.10 - Gaps on sophisticated protection	All

Table 16 provides a binding between identified threats, relevant assets and gaps/challenges in this section.

Table 16: Mapping Assets, Threats and Gaps

Threat Group (TG)	**Threat (T)**	**Asset (A)**	**Gaps (G)**
Unintentional damage (1)	Security misconfiguration (1)	Interfaces, Security Techniques	G5.1 G5.2 G5.3 G5.5 G5.7
	Inadequate design (2)	All	G5.2 G5.3 G5.7 G5.8
Interception and unauthorised acquisition (2)	Interception of information (1)	Data, Interfaces, Security Techniques	G5.1 G5.2 G5.3 G5.7
	Sensitive data exposure (2)	Data, Security Techniques, Roles	G5.1 G5.2 G5.3 G5.4 G5.5 G5.7
Nefarious activity/abuse (3)	Broken authentication and access control (1)	Data, Security Techniques, Roles	G5.1 G5.2

			G5.3 G5.4 G5.7
	Denial of service (2)	Data, Interfaces, Security Techniques, Roles	G5.3 G5.4 G5.7 G5.10
	Code execution and injection (insecure APIs) (3)	Data, Interfaces, Security Techniques	G5.1 G5.4 G5.7
	Insufficient logging and monitoring (4)	Data, Interfaces, Security Techniques	G5.3 G5.4 G5.7
	Untrusted composition (5)	Interfaces	G5.3 G5.4 G5.7
	Supply-chain security (6)	All	G5.6
	Virtualization (7)	Data, Interfaces	G5.3 G5.6
Legal (4)	Violations of laws or regulations (1)	All	G5.7 G5.9
Organizational threats (5)	Malicious insider (1)	Application Security, Data, Platform Security, Roles	G5.9 G5.10
	Skill shortage (2)	All	G5.7 G5.9

3.8. User-Centric Security

3.8.1. Threats (from D4.1)

In this section we provide a summary of the threat categories identified in D4.1 in domain user. Before introducing the major characteristics of the threat taxonomy, a note of caution should be presented because the User domain, of all the cybersecurity domains, is the more recent to be considered as a primary domain of concern and, for this reason and also for the non-technical nature of many related aspects, its scope is still somehow debated or sometimes ambiguously defined. For example, still few years ago, the Health Information Trust Alliance stated that "cybersecurity does not address non-malicious human threat actors, such as a well-meaning but misguided employee." [24] This means that at least, for a relevant organization in one of the key industrial sectors, human errors were largely out of the scope of cybersecurity. This would be inconceivable with respect to current cybersecurity analyses, after the User domain has been elevated at the same level of traditional cybersecurity domains such as Systems, Networks, or Data.

On the other side, it is not uncommon today to encounter articles on online cybersecurity-related magazines and in surveys making claims such as "malicious insiders [...] and human error [...] to be the two top cybersecurity threats".[159] These claims, together with the utterly misleading logical fallacy of considering users (or the human factor) as threats (as well as the too often repeated analogy, in technical circles, between users and the weakest link in a chain), grossly overstated and confound threats connected with the User domain, with the aim of shifting the attention of organizations and professionals to the newest hype. Click-baiting editorial styles or commercial interests are likely part of the motivations for such

[159] Human Factor is a Persistent Cybersecurity Threat, Survey Says. *Security Magazine*, August 2019. https://www.securitymagazine.com/articles/90734-human-factor-is-a-persistent-cybersecurity-threat-survey-says

poor information, but a general lack of understanding and experience with studies on human errors and user behaviour connected to IT technologies is equally an important factor.
However, these anecdotes should remind of the fact that the boundaries and the threats of the User domain are still to be regarded as, to some extent, subjective and not yet well established.
More thoroughly conceived and articulated analyses have appeared in recent years raising the attention to the human factor in cybersecurity. For example, NIST, through the Federal Information System Security Educators' Association (FISSEA), has concluded that human errors and negligence often play an important role in the chain of events leading to data breaches. Also, security risk management and business operations are often disconnected functions, resulting in a poorly coordinated process management.[160] The Verizon Data Breach Investigation Report (DBIR)[161], a respected annual survey, for the current 2019 edition confirms that the category *Miscellaneous Errors*, while not among the most relevant for security incidents (i.e., security events not resulting in data breaches, such as Denial of Services), it is instead one of the lost likely pattern for data breaches. Interestingly, other categories that could be partially referred to the User domain, such as *Privilege Misuse* (e.g., employees using their system and data access privileges outside their job duties) and *Cyber-Espionage* (e.g., this threat category often adopt deceitful techniques to target specific employees or make use of unfaithful insiders), are relevant. Such results hardly represent a surprise, in fact their relevance is a fact from years.
Many have debated about the importance of the organization for cybersecurity and, to this regard, the expression *Human-centered security* has been used. Holz et al. [25] have presented a detailed research agenda aimed at reorganizing industrial processes of cybersecurity around the role of individuals in all their forms, as software developers, IT integrators, system administrators, and end users. Many others, for instance ENISA[162], Corradini and Nardelli [26], and Safa et. al. [27] have addressed the security threats related to users focusing on the perceived need of more and better training of the workforce. The lack of adequate training programs and curricula for cybersecurity professionals as one of the main reasons for the gap in available workforce is widely debated worldwide and the subject of several proposals [28] [29] [30].
Regarding cybercrimes, the User domain is more specifically concerned with identifying who is responsible, which characteristics they exhibit, and their main motivations and pattern of activity. Two large profiles have emerged in recent years: criminal organizations and state-sponsored groups; the former mainly responsible for financially motivated crimes, the latter mainly driven by cyber-espionage and data breaches. Criminal groups exploit vulnerabilities in existing technologies, as well as the features offered by new technologies, engaging in the traditional arms race with law enforcement and companies' prevention and mitigation solutions. State-sponsored attacks are often framed with reference to cyberwarfare [31] [32]. Despite that reference could be reasonable in certain situations and for specific contexts, however, it often confounds the analysis by focusing more specifically on geopolitical and military issues than on more operational and business-related threats [33]. State-sponsored attacks are mostly related to cyber-espionage; thus, they represent a lucrative activity for the perpetrators and, often, a severe competitive loss for the victims

[160] Cybersecurity – the Human Factor: Prioritizing People Solutions to improve the cyber resiliency of the Federal workforce. *FISSEA*. 2017. https://csrc.nist.gov/CSRC/media/Events/FISSEA-30th-Annual-Conference/documents/FISSEA2017_Witkowski_Benczik_Jarrin_Walker_Materials_Final.pdf
[161] Verizon Data Breach Investigation Report , https://enterprise.verizon.com/en-nl/resources/reports/dbir/2019/introduction/
[162] ENISA, *Cyber Security Culture in organisations.* February 2018. https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

[34] [35] [36]. Therefore, they should probably be more conveniently framed with respect to international market competition and the protection of strategic investments.
Finally, we mention two classes of threats that still are not commonly included in cybersecurity threat taxonomies: threats to a company's market share and threats from amplification effects on media. Analyses of the economic and financial consequences of a security breach have been studied for a long time [37] [38] [39] [40]. However, it is still an issue that this 2x threats has not entered the cybersecurity mainstream and requires more and better detailed analyses. In some cases, the actual negative effects, especially long-term effects, have been questioned, on the basis of the complex and non-linear cause-effect relationships governing stock prices [41] [42] [43].
The amplification effect of media, traditional or online, with respect to risks and threats is a well-known effect that is still largely ignored in cybersecurity threat taxonomies. On the opposite, it is important to consider, at least as one of the new threat sources to put on a watch list. Episodes where the social amplification of risks, driven by the media, have had relevant effects are discussed in the literature [44] [45] [46] [47].

In summary, a threat to User assets can be considered as *"any circumstance or event that produces adverse effects primarily on individuals as part of an organization or as stakeholders. The threat should be carried out through digital means, either voluntarily (attack/cybercrime) or involuntarily (human error)"*. The threat taxonomy is composed of the following groups:

- TG6.1 – Human errors: This group includes all threats causing unintentional information leakage or sharing due to human errors.
- TG6.2 – Privacy breaches: This group includes all threats causing privacy breaches.
- TG6.3 – Cybercrime: This group includes all threats due to data/model poisoning and aiming to picture a scenario that does not adhere to reality.
- TG6.4 – Media amplification effects: This group includes threats coming from nefarious activities. It requires active attacks targeting the infrastructure of the victim, including the installation or use of malicious tools and software (see Appendix A.6 for more details).
- TG6.5 – Organisational threats: This group includes threats to the organizational sphere.

3.8.2. New Threats and COVID-19

COVID-19 has mainly amplified existing threats for the user-centric domain, while introducing new gaps and challenges that are discussed in the next section.

3.8.3. Gaps and Challenges

In this section, we provide an overview of the gaps and challenges relevant for the user-centric domain and discuss the opportunities for future research.

In short, the main open issue and challenges related to the user-centric domain of cybersecurity is that, within the community of scholars and professionals, there is still a generalized lack of knowledge, experience and thus agreement, about how to deal with security problems whose root causes have behavioural origins, which methodological approaches are best-suited to analyse and contextualize user-centric threats, how to predict, measure, and evaluate the outcome of mitigating activities and countermeasures, and overall how to reason about cybersecurity threats and attacks with human and technological aspects

in a thoroughly and unified way. Way too often, user-centric and technological domains of cybersecurity have been approached as distinct aspects and knowledge domains by experts sharing very little in their background and expertise and throughout approaches frequently are inconsistent with each other. All of this has dramatically reduced the ability of the cybersecurity field to analyse threats and possible solutions, to be adaptive with respect to the high heterogeneity, time dependence of threats, security landscape, and to truly absorb key concepts from important fields like risk analysis and management, stochastic modelling and analysis, network science and behavioural studies, (social) media studies as well as control theory and computational social sciences studies. These are all examples of well-established scientific disciplines and areas of studies that have developed a large body of knowledge related to individual and social behaviour, which may shed a light on many cybersecurity aspects still poorly analysed and offer robust methodological approaches, as well.

For example, ransomware is one of the most dangerous cybersecurity threats for industries like manufacturing or healthcare and often the point of entry for the malware is a phishing email. This could happen despite the fact that phishing and in general email threats, is one of the oldest and best-known cybersecurity threats, certainly not an obscure 0-day for which almost everybody has never heard of. Phishing is perhaps the first threat presented in awareness programs, which is easy to grasp by journalists and often mentioned in headlines, it is a looming danger that everybody knows about. Nevertheless, despite the fact that security surveys consistently show a steady decline in the rate of employees of major corporations that tend to fall victims of phishing emails, ransomware driven by phishing emails seem almost unstoppable and, systematically even seemingly tech-savvy companies end up paying the ransom to cybercriminals as their last resort in order to recover operations. The rise of ransomware and the apparently unsolvable problem of phishing emails cannot be fully understood without a detailed understanding of the organization practices and behavioural responses of employees to rare events. The whole area of human errors, so relevant for cybersecurity, could be fully analysed only from a user-centric perspective and a specific understanding of the context, like working conditions and relations.

Another example of partial understanding of a problem due to insufficient analysis from a user-centric perspective regards the still vague and uncertain methodologies to carry out a cost/benefit analysis of cybersecurity technologies and solutions. How to evaluate benefits, in particular, is mostly based on presumed well-suited metrics (e.g., in the definitions of KPIs, control dashboards) rather than on detailed measurements, testing, simulations, longitudinal experiments, multivariate stochastic analysis etc., i.e., the whole body of knowledge that has been developed in the past in order to manage uncertainty in decision making. It still is a rare event to see cybersecurity projects fully embracing such classical methodologies for making estimates.

The same lack of integration between user-centric disciplines and cybersecurity is reflected on the ongoing debate about the skill shortage in cybersecurity, the professionalization of the cybersecurity expert profile and the reputed need of education curricula. Those new cybersecurity curricula should be, at the same time, more detailed with respect to the competences and encompassing a much larger range of skills and disciplines than traditionally considered. While such efforts have evident motives to be pursued, the vagueness and inexperience in reasoning about behavioural and social skills is manifest in the fact that it is still unclear whether cybersecurity should aim to include into its domain of knowledge parts of behavioural and social disciplines, or vice versa it should become part of disciplines like risk analysis, management, labour studies, behavioural studies, or otherwise it is the mutual interdependence between knowledge domains that should be fostered as something new for these fields.

In the following, we list some of the main cybersecurity user-centred gaps, with a summary.

User Domain-Specific Gaps and Challenges

G6.1 - Gaps on modelling user behaviour. One challenge in cybersecurity that is still looming unaddressed from decades of discussions in academic and professional circles, is how user behaviour, relevant to cybersecurity, should and could be modelled with the twofold aim of reducing the frequency of errors and preventing cascade effects and, on the other hand, of forecasting threats likelihood which depend on user behaviour. Attempts at developing behavioural analyses and features, for example in early 2000s with Host-based Intrusion Detection Systems (HIDS) or with the application of Artificial Intelligence techniques have produced interesting prototypes, but never achieved the sufficient level of maturity to be deployed as robust solutions. From a different perspective, research on human errors has a long and fruitful history, e.g., in transportation or for critical systems, but a true integration with cybersecurity issues mostly for the most part in its early stages. Regarding behavioural studies, they represent a rich research field, especially in psychology, sociology, and economy, but again, a convergence with cybersecurity never truly happened, other than a superficial characterization of the so-called "hacker mindset" or adversarial thinking.

G6.2 - Gaps on the relation between user behaviour and adverse security-related effects. There is a lot of studies regarding phishing in the past decades. Equally, testing for employees' likelihood of falling victim of a social engineering scam through phishing has become a common measure in the security arsenal of security-conscious enterprises. The positive effects of efforts directed to mitigate phishing threats are clearly visible in statistics about the frequency of clicking on a malicious attachment or link: the rate of enterprise users likely to click has dropped considerably (down to few percentage points). So quantitatively, we are certainly better off and the number of social engineering cases have dropped during the years. But, what about qualitatively? Qualitatively, it is a different story and social engineering, phishing, then ransomware attacks have not decreased in relevance. On the contrary, they all have increased their relevance, despite the number of cases having dropped. The fact that it was not clearly and properly understood in the past is that phishing, social engineering, and in general user-centered threats should not be counted, they should be weighted. The sheer decrease in the number of phishing cases had the result of reducing the most obvious cases; those grotesque phishing campaigns that were commented on in countless reports, those half-translated emails produced by botnets. However, those cases, as it turned out, were just the low-hanging fruits easy to pick with a decent awareness program and when experience accumulated even among less tech-savvy employees. The real difficult cases remain, those that even less in number have an enormous potential to wreak havoc, for the dire consequences that may produce, from halting the operations of critical health divisions, or the production line in manufacturing, or tricking top C-level individuals into disastrous decisions. The problem now is that these remaining critical cases are not mitigated with past solutions and often companies and organizations find themselves defenceless.

G6.3 - Gaps on security information. This is one of the most recurrent in cybersecurity: data and knowledge about the threat landscape are scarce in quantity and poor in quality. On the one hand, a consequence of this is to endlessly replicate the same questions, the same uncertainties without establishing, or doing that with difficulty and insufficiently firm points in the analysis of the context. Large uncertainty still looms about the relative importance between internal and external sources of attacks, about the type and nature of main threats

and about how to rank threats and vulnerabilities. For all these issues, apparently, the analyses start from the beginning, over and over. Same for what concerns data and knowledge sharing among subjects equally exposed to cybersecurity threats, like companies of the same industry or country, public organizations, agencies, or departments. Data and knowledge sharing still flow with great difficulty and poor quality, with the result that a comprehensive picture and a shared awareness build up slowly and partially. One evident gap, with this respect, is in the ability to assess the quality of reports and surveys, which seems on average low, with the result that good quality analyses coexist with poor ones, sometimes both referred as equally informative.

G6.4 - Gaps on security training and education. There is a well-known fact that there is a gap between the number of competent and skilled professionals requested by the industry and the number of people enrolled in academic-level cybersecurity training programs. What is less known, though, is that clear remedies are lacking too, because, in short, there is no agreement about what an adequate cybersecurity education should be and who should be in charge of. Proposals range from the extreme positions of those envisioning young teen-agers enrolled in cybersecurity programs to those that consider cybersecurity a specialist topic to be addressed in advanced studies. Between these two boundaries, almost all proposals have achieved some sort of recognition, from Computer Science/Engineering to Law and Management cybersecurity programs, academic training vs. specialist certifications, hands-on vs. theoretic approaches, corporate in-house or college grade training. In addition to these options, all implemented and sustained in some circles, the most difficult question is about content. What should be considered required knowledge for the cybersecurity workforce? What supplementary knowledge? How to define coherent curricula? For such questions, several approaches have been attempted. More recently, the consensus seems to lay towards a large set of competences, not just strictly technical but including many disciplines. While the idea of a comprehensive and multidisciplinary education has certainly many reasons to be promoted for modern cybersecurity experts, nevertheless the doubt persists that, ultimately, it would lead to unrealizable proposals, heterogeneous superficial programs that will touch upon many issues without teaching and a general sense of vagueness of a professional profile without a characterization.

G6.5 - Gaps in collaborative protocols for disclosure. Another user-centred area that clearly shows a gap is in the collaborative protocols governing how vulnerabilities should be assessed and disclosed. Vulnerability disclosure procedures have been a hot topic for many years, despite the fact that its actual relevance was uncertain. Despite the many discussions, however, a clearly agreed procedure has never been established between the community of security researchers and software companies or organizations.
However, in relatively recent years, two new events seemed to be able to change the course of this seemingly endless debate: the raise of bug bounty programs and the standard ISO/IEC 29147:2018 Information technology — Security techniques — Vulnerability disclosure. Bug bounty programs brought high expectations for a brand-new era of vulnerability discovery and disclosure. Finally, the work looked perfectly regulated and rewarded, getting rid of the conflicts that characterized the relations between security researchers and companies. The business-oriented approach introduced by bug bounties seemed to work, at least initially. However, old and new problems emerged quickly. The problem of reward was not settled, with black, grey and white vulnerability market still offering an alternative to bug bounties. Then other problems re-emerged, with respect to the type of vulnerabilities, the degree of freedom the researchers could enjoy, and the effectiveness of the approach, apparently biased towards low-hanging repeatable

vulnerabilities and possibly mismanaged by vendors. As a consequence, the enthusiasm for bug bounties cooled down and today they are seen as a problematic approach.
For what concern the ISO standard, its appearance brought the idea that if ISO stepped into the matter, then companies would follow, and the issue of vulnerability disclosure would have finally managed as one of the other information security and management processes. Unfortunately, up to now, almost nothing has materialized, except some initiatives by international organizations, without any real effect. The ISO 29147 standard essentially lays almost abandoned and useless without any real support from industries. Therefore, the problem of how to govern the vulnerability disclosure process still persists, barely addressed in public, while, for a remarkable part, it becomes the core business of a, not rarely, murky industrial sector.

Gaps and Challenges in the Era of COVID-19

With respect to the current COVID-19 pandemic, it comes with no surprise that criminals have repeatedly tried to exploit the state of fear, uncertainty and doubt that many individuals have and still are experiencing. The infamous FUD triple (fear, uncertainty and doubt) that has been for a long time the main driver for cyber security investments, has made an unexpected return with the coronavirus, as a common feeling in society. As it already happened in the past, in the aftermath of dramatic events or existential threats (e.g., wars, past pandemics, economic crises, insurrections, or disasters), there are scammers ready to profit from people in a state of distress, feeling threatened, worried for relatives and desperately looking for remedies or healing. It has been documented that physical and movement restrictions, closures of workplaces and all the uncertainties that the COVID-19 has brought have produced a spike in depression symptoms and condition of psychological distress [48] [49].
Cyber criminals have carried out a whole lot of well-known online scams during the pandemic months of 2020. None of them is surprising or present any novel features. It is the usual arsenal of phishing email campaigns, fake products, fraudulent advertising and preposterous pseudoscientific theories. Google has organized awareness campaigns through the website https://safety.google/securitytips-covid19/, where safety tips are given with regard to the most likely scams and prudent online behaviour. The categories of scam listed by Google are: Fake healthcare organizations; malicious web sites falsely offering personal protection items urgently sought by individuals (e.g., face masks, hands sanitation products, etc.); scammers presenting themselves as representatives of governmental agencies (e.g., the tax revenue office); false financial offerings directed to people suffering harsh economic conditions; false donation campaigns for humanitarian support.
Europol has created a similar web page for COVID-19 shopping scams[163]) and another more comprehensive about safety tips[164] On this site the overview about the intersection between COVID-19 and criminal activities is broadened with respect to the few Google's tips. Europol reports cover the increase of sex offending and online child abuses cases, the response of drug markets to the new conditions during physical restriction periods, the spread of counterfeits, and the spread of disinformation campaigns. A bleak scenario is the one emerging from the Europol reports[165], much worse than "simple" online scams highlighted by Google. The European Commission took notice too of the increased threat level to European citizens due to scams and, through its Consumer Protection Cooperation

[163] https://www.europol.europa.eu/covid-19/covid-19-shopping-scams
[164] https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know
[165] INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020", European Union Agency for Law Enforcement Cooperation, 2020. Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

Network (CPC) arm, published its own website dedicated to scams and rogue traders during the COVID-19 pandemic.[166]

Cross-Cutting Gaps and Challenges

As for several other security domains, the increase of complexity in dealing with security problems and often inadequate approaches to tackle it there are some of the main cross-cutting gaps. A renewed attention for user-centered issues is brought by the same development that makes network, IoT and application issues, even more relevant and difficult to deal with. The overall scenario expanded globally the interconnection covers all continents and criminal groups of even remote villages in the periphery of main countries are able to mount successful user-driven attacks and frauds. The rise of social networks and media has multiplied communications and interactions, also introducing new means and style of communicating, which bring their peculiar threats. New laws and regulations, especially for privacy matters, have considerably changed how certain security problems are governed, with effects on a number of security dimensions. Next, technological trends have produced cross-cutting gaps. It seems a distant past those days when a security perimeter of a company was a clearly well-defined concept, as well as when devices inside the perimeter could be strictly controlled and the difference between personal and working devices was clear to all. Now the situation has changed, considerably. The perimeter is fluid, BYOD is the norm and remote working is on course to be the next reality. These changes, once again introduce cross-cutting gaps in knowledge, methods, skills and solutions, stemming from network management to user management.
For the most part, they point to the ability to tackle different security domains at the same time, cohesively. Decision support systems, once the domain of optimization techniques, will probably become more fuzzy, stochastic and risk oriented. The ability to adaptively change the decision support system to new information and knowledge will perhaps become more crucial than optimization. In this scenario, the interface between human and algorithmic support is critical. We have already observed how unaccounted algorithmic solutions too often lead to unacceptable, unethical, and ultimately damaging outcomes for society. One of the big challenges ahead of us, for cybersecurity too, is certainly how to make it possible to have both algorithmic and human decision support and assessment.

Table 17 shows how the gaps in the user domain affect the other domains of interest of CONCORDIA.

Table 17: Cross-Cutting Gaps

Gaps	**Additional Domains**
G6.1 - Gaps on modelling user behaviour	Data, Network
G6.2 - Gaps on the relation between user behaviour and adverse security-related effects	Data, Network
G6.3 - Gaps on security information	Data
G6.4 - Gaps on security training and education	All
G6.5 - Gaps in collaborative protocols for disclosure	All

Table 18 provides a binding between identified threats, relevant assets and gaps/challenges in this section.

[166] https://ec.europa.eu/info/live-work-travel-eu/consumers/enforcement-consumer-protection/scams-related-covid-19_en

Table 18: Mapping Assets, Threats and Gaps

Threat Group (TG)	Threat (T)	Asset (A)	Gaps (G)
Human errors (1)	Mishandling of physical assets (1)	All	G6.3, G6.4
	Misconfiguration of systems (2)	All	G6.3, G6.4
	Loss of CIA on data assets (3)	All	All
	Legal, reputational, and financial cost (4)	All	All
Privacy breaches (2)	Profiling and discriminatory practices (1)	External	All
	Illegal acquisition of information (2)	All	All
Cybercrime (3)	Organized criminal groups' activity (1)	Data, Security Techniques, Roles	G6.2, G6.3, G6.4
	State-sponsored organizations' activity (2)	Data, Interfaces, Security Techniques	G6.2, G6.3, G6.4
	Denial of Service (3)	Data, Interfaces, Security Techniques, Roles	G6.3, G6.4
	Insufficient logging and monitoring (4)	Data, Interfaces, Security Techniques	G6.2, G6.3, G6.4
	Untrusted composition (5)	Interfaces	G6.3, G6.4
	Supply-chain security (6)	All	G6.1, G6.2, G6.4
	Virtualization (7)	Data, Interfaces	G6.3, G6.4
Media amplification effects (4)	Violation of laws or regulations (1)	All	G6.1, G6.2, G6.4
Organisational threats (5)	Malicious insider (1)	Data, Application Security, Platform Security, Roles	G6.1, G6.2
	Skill shortage (2)	All	G6.4

3.9. Key Takeaways

This section summarizes the most important findings, as key takeaway, emerging from the gap analysis carried out in this deliverable.

- **Extended attack surface.** The attack surface is continuously expanding, despite the emergence of innovative security platforms, innovative technologies, organizational and regulatory initiatives in the field. The advent of 5G, IoT, smart working, the huge amount of the new vulnerabilities discovered every day actually put an enormous effort on the security departments and their experts to prevent, or at least to contain and mitigate the threats.
- **COVID-19 as an amplifier of threats and attacks.** COVID-19 pandemic has tangled even more the situation in terms of increasing scams, SPAM, ransomware and disinformation. This evolving scenario stresses the importance of the capacity to perform security prevention and operations in an effective manner. Possible solutions could be based on more automation of current processes, investigation about the application of Artificial Intelligence algorithms and last but not least training and education.
- **Security management.** The full adoption of mature security processes (such as patch management, vulnerability management, PSIRT, Governance, risk management and compliance (GRC) and so on) are still far to come. Despite the availability of proper tools and products, fully documented standards and

procedures, well prepared security experts, the management of the security processes still remains a very hard task to be properly deployed inside main organizations, due to possible impacts on other processes and systems operations and legacy systems. Also, in this context automation and AI/ML could help to improve the correctness and reduce complexities. In this context the identification and adoption of a novel way to address this hardening/patching processes, reducing the operation impacts, could be of real value.

- **Interoperable Data Protection.** The need of extending data protection to hybrid and complex distributed systems, require the need of designing and implementing new data protection approaches that address the peculiarities of hybrid systems mixing heterogeneous components, from cloud/edge nodes to smart devices and minuscule sensors. In addition, these approaches must address an increasing number of regulations and policies, which may model conflicting requirements.
- **Data (Un)Trustworthiness.** The increasing migration from code to data, especially in application areas where it is easier to collect samples that embody correct solutions to individual instances of a problem, than to design and code a deterministic algorithm solving it for all instances, made the role of data pivotal. At the same time, the increasing development of autonomic and adaptive systems pose strong requirements on the quality of data. Data trustworthiness is a fundamental challenge that needs to be addressed to increase the precision of modern system behaviours.
- **ML/AI Verification.** Today, in many critical domains and application scenarios, the behavior of modern IT systems depends on the behaviour of machine learning models composing them. These models are often treated as black boxes, thus making automated decisions based on inference unpredictable. We are witnessing a migration from traditional software systems based on deterministic algorithms to systems where ML models reason on data to calculate a solution to individual instances of a problem. In this context, the need of verifying the non-functional properties of ML models, such as, fairness and privacy, becomes fundamental to provide trustworthy system and services with certified ML-based behaviour.
- **Complexity**. Applications are miniaturized, distributed and managed by complex orchestration platforms. In this scenario, security management is more difficult, involving orthogonal aspects such as authentication, authorization, securing network communication. Also, supply-chain security must be taken into account, since a compromise or a vulnerability can come from one of the many components (hardware, library, etc) forming a system.
- **Long-standing issues**. While microservice-based architectures have established themselves as the de-facto standard for backend applications, there are still long-standing issues to be solved once and for all. In fact, despite the recent advances (programming languages, tools supporting programmers), security and safety by default are far still far to come. For instance, many malwares still take advantage of memory bugs, and web applications still suffer from poor security and coding practices.
- **Management of Human Errors.** The ability to understand, predict and mitigate human errors is compromised by the persistent lack of reliable models of users' behaviour.
- **Limited Knowledge.** The persistent lack of high-quality data and information about on-going security threats harms analysis capabilities and reduces knowledge sharing.

- **Professionals Shortage.** Many uncertainties still remain regarding the professionalization of security experts, including the definition of specific curricula, skill profiles, and education programs.
- **Skills and education**. Complex applications and sophisticated threats require skilled personnel to deal with. Strong solutions building on security processes, which go beyond mere technical aspects, should be introduced. At the same time, the ever increasing usage of digital technologies to carry out day-to-day activities, a trend pushed by the COVID-19 Pandemic, demands for the digital education of everyone, to take full advantage of what technologies offer and, also, to protect them from targeted attacks.
- **User Negligence and Misconfiguration**. The remote users should undergo training on security topics including phishing, password guidance, and privacy screen, device hardening, working with confidential materials, and securing physical computing assets in order to mitigate related cybersecurity risks. Special emphasis should be put on the cloud services configuration and change of control since misconfiguration can potentially leak sensitive data and cause irreversible damage.
- **Logistic Challenges Resulting from the Service Overload.** Due to the ever-increasing usage of cloud and streaming services, cloud service providers are facing issues related to the networks and resources. As a result of unexpected overload and insufficient hardware, service and availability of those services are becoming increasingly difficult to maintain. In order to solve this issue, cloud service providers should work on improving their infrastructure. Moreover, to prevent the potential security hazards coming from DDoS attacks, cloud service providers should work on stopping large quantities of cloud server traffic by thoroughly checking, absorbing, and scattering DDoS attacks.
- **Lack of Standards.** Cloud environment services should adopt universal standards regarding the interoperability solutions and cloud transparency is SLAs for the sake of ensuring compatibility between independent systems. On the other hand, users and organizations should be aware of which cloud service providers meet the necessary industry standards to avoid potential censures and fines.
- **Cloud Transition Requirements.** Users/organizations have to ensure that they meet the necessary data storage and security protection requirements, in order to allow for the secure transition. Appropriate control planes should be used to empower necessary security, integrity, stability and data runtime. Furthermore, cloud services' security can depend on the design of the user interfaces and APIs, which act as gateways to the cloud. Hence, in order to diminish the security vulnerabilities, the user interfaces and APIs have to be designed with security considerations in mind.
- **Careful adoption of new technologies.** New technologies especially in emerging domains such as Device/IoT, provide a number of positive effects on system security but also can expose to severe side effects. Specifically, if the adoption is not correlated with adequate planning, the negative effects can be much more relevant than the positive ones. For instance, there is a clear need to have time to design the solution including new technologies in order to check security implications also in terms of integration/interoperability with the rest of the system to be protected. There is also the need to acquire the right competencies and skills both to deploy and implement the new solutions but also to reverse such competences to the personnel that have to work with such new technologies in operation. The effect of not being capable to understand this key concept was clearly underlined by the pandemic where the need to react rapidly to an emergency have almost excluded the

possibility to plan training and acquire adequate skills to operate with the new devices exposing the entire system to severe security threats.

- **Reinforce diagnosis and remote management.** Most of the IoT issues refer to the lack of a secure and fully functional remote management procedures allowing to patch, check configurations and assure behaviour of any IoT devices without requiring to physically operate on them. This will also help in removing physical accessible interfaces and introducing secure boot functionalities removing the need to have weak authentication and authorization procedures.

3.10. Dissemination material

Dissemination material is important to make the content of this deliverable popularly available (e.g., blog posts, white papers). Following activities done in Y1 and Y2 related to D4.1, we are preparing the following documents:

1. An HTML version of the gaps and challenges in this deliverable to simplify browsing by readers.
2. A report on top findings and key takeaways on gaps and challenges.
3. A blog entry on the impact of COVID-19 on cybersecurity threats.

4. Legal Perspectives

This Chapter elaborates on cybersecurity from the various legal and policy perspectives. To this end, the discussion below does –primarily- four things. First, in line with the rationale pursued under the technical perspective, it produces a regulatory mapping illustrating how currently applicable regulations relate to the domains of interest previously defined. Second, it provides an overview of the latest developments pertinent to the regulatory landscape, initially captured under the first edition of the Threat Analysis Report (D4.1), delivered in Year 1 of the project. Third, based on input gathered directly from consortium partners, the discussion below summarises in a concise manner challenges encountered linked to the implementation of cybersecurity, also, through daily organizational practices. Finally, the Chapter produces an early set of recommendations aiming to contribute to bridging the gaps between the "state of play" of cybersecurity and the "state of the art", also, envisioned through newly adopted and other -possibly- forthcoming regulations within EU.

As mentioned previously, the discussion below is largely based on desk research, but also on inputs gathered from a set of qualitative interviews conducted with representatives from CONCORDIA pilots, as well as other selected partners. Furthermore, the discussion below elaborates on the impact of COVID-19 both with respect to the emerging policy considerations, as well as with respect to pre-existing organizational cybersecurity practices, which were -to an extent- challenged and could be, thus, improved.

4.1 Regulatory Mapping

Drawing upon the domains of the working groups identified under Task 4.1, this section attempts to map the currently applicable regulations at EU level with the focus areas identified, meaning, networks, systems, data, applications and protection of end-user. To this end, the mapping captured in the table below was based on the articles providing for the subject matter and 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).

Table 19: Applicable EU regulations and technology domain of interest[167]

Cyber security cOmpeteNCe fOr Research anD InnovAtion CONCORDIA

REGULATION IN DIGITAL AGE	NETWORK	SYSTEMS	DATA	APPLICATION	PEOPLE
NIS Directive	✓	✓		Impact-Based?	
Cybersecurity Act	✓	✓	✓	✓	?
Free Flow of Non-Personal Data Regulation		✓	✓	✓	✓
General Data Protection Regulation	✓	✓	✓	✓	✓
Product Liability Directive	?	?	?	?	✓
Radio Equipment Directive	✓	✓	✓	Impact-Based?	
eIDAS Regulation	✓	✓	✓	✓	✓

Overall, even by looking strictly into the scope of the currently applicable regulations as reflected above, it can be seen that European regulators have provided for all domains of interest identified in Table 19. As surfaced earlier, the regulations in place assign concrete obligations to the responsible actors identified in each case, for example, of risk management. Nevertheless, it could be argued that the large-scale adoption of technologies, hyper-connectivity, the complex structure of the supply chain, both upstream and downstream, does raise concerns in relation to the clear determination of the liabilities incurred (also, on the basis of contractual arrangements) and, in essence, on the actual effectiveness of the law. Notably, the issue of liability in the cyberspace, also, within the field of cybersecurity and the associated insurance mechanisms in place has been -to an extent- addressed under D4.1 1st Year Threat Analysis Report.

4.2 Update on the Existing Regulatory Landscape

This section provides an overview of updates and developments concerning the EU Regulatory Landscape that have transpired since the publishing of the first edition of the Threat Analysis Report (D4.1) [168]. As was done in corresponding section of D4.1, this section deviates from the approach taken in other parts of the present document of structuring the discussion based on the separate thematic areas, meaning, the "network-centricity", the "system-centricity", the "data-centricity", the "application-centricity" and the "end-user centricity" and instead discusses the legal aspects of cybersecurity in a rather holistic manner. The discussion below revolves only around the most relevant pieces of legislation and it, therefore, does not provide for a comprehensive presentation of all EU regulations that could be deemed relevant for cybersecurity.

[167] Due to the fact that at the time of drafting this deliverable, the Product Liability Directive was under review, the implications of the Directive in relation to the domains of interested is yet to be seen. The identification of the exact domains to be covered by the revised Directive, therefore, remain to be seen.

[168] Given that no significant development has taken place for the Revised Payment Services Directive that is relevant for the current deliverable, the said Directive has been not included in the discussion in Section 4.2

Notably, in the last year, adoption of new technologies has grown in manifolds especially due the COVID-19 pandemic. This, in addition to other factors, prompted EU authorities to evaluate the relevance of various existing legislations in line with the evolving landscape while also introducing new initiatives, publishing guidelines and conducting public consultations on multifarious topics including cybersecurity. More specifically, even at the time of finalising this deliverable (first half of December 2020)- the European Commission published a series of policy making documents and legislative proposals, including the new EU Cybersecurity Strategy[169], the revised Directive on Security of Network and Information Systems (NIS 2 Directive)[170], the proposal for the Digital Services Act[171] and the Digital Market Act[172] and the Staff Working Report on the impact regarding Cybersecurity of 5G networks[173]. Due to the overlap in timing, these updates have not been captured in the present deliverable. As mentioned earlier, though, these developments will be discussed under the subsequent deliverable i.e., D4.3: 3rd Year Report on Cybersecurity Threats.

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

The Directive on security of network and information systems[174] (NIS Directive) aims at enhancing cybersecurity across the EU and is also the first piece of EU-wide cybersecurity legislation. To briefly encapsulate the elaborate overview under D4.1, the NIS Directive requires operators in critical sectors (such as banking, health, finance, transport) and enablers of information society services (such as app stores, social networks and search engines) to implement effective risk management practices. It also requires Member States to set up at least one Computer Security Incident Response Team (CSIRT) that will be responsible for monitoring threats and incidents at a national level and to create appropriate response mechanisms. At an EU level, the Directive establishes a Network of the national Computer Security Incident Response Teams (network of CSIRTs) to build trust and confidence between the Member States and enable effective communication.

The healthcare sector which falls within the scope of the Directive has been majorly impacted by the COVID-19 pandemic and have witnessed a surge in phishing campaigns as well as ransomware attacks. The cyberattack on Brno University Hospital in Czech Republic in March 2020 forced the hospital to shut down its entire IT network and to relocate patients to other hospitals. [175] Other such similar attacks in hospitals and related organisations in different Member States have caused a stir in the healthcare community.

[169] Joint Communication to the European Parliament and the Council, The EU's Cybersecurity Strategy for the Digital Decade, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72164

[170] 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, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=72166

[171] 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://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608117147218&uri=COM%3A2020%3A825%3AFIN

[172] 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://eur-lex.europa.eu/legal-content/en/TXT/?qid=1608116887159&uri=COM%3A2020%3A842%3AFIN

[173] ENISA Threat Landscape for 5G networks, available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks/at_download/fullReport

[174] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union OJ L 194

[175] Czech hospital hit by cyberattack while in the midst of a COVID-19 outbreak, available at https://www.zdnet.com/article/czech-hospital-hit-by-cyber-attack-while-in-the-midst-of-a-covid-19-outbreak/

[176] Through the CSIRT network, which was established pursuant to the NIS Directive, enabled Member States to continuously exchange information and issue situational reports together with the EU Institutions.[177]

Given that since its enactment, the cyber-threat landscape has been constantly evolving and becoming more widespread, the European Commission published an initiative involving the review of the NIS Directive.[178] Based on evidence gathered, the Commission is of the view that while the NIS Directive immensely contributed to improving the cybersecurity capabilities within the Member States, there were various issues relating to its implementation.[179] Firstly, due to the minimum level of harmonisation and the identification process applicable to operators of essential services, Member States have given a lot of discretion which has resulted in fragmentation in the regulatory landscape and several inconsistencies. This has also resulted in various sectors and actors with critical societal and economic activities and which are susceptible to cyber risks to be left outside the scope of the Directive. Hence, to achieve a "Europe fit for the Digital Age" as envisioned by the European Commission, the Initiative aims to identify suitable policy options including non-legislative measures and possible regulatory interventions, as well as a combination of the two.

The European Commission recently sent out reasoned opinions[180] to Belgium, Hungary and Romania referring to their failure to comply with their obligation set out in the Directive on security of network and information systems (NIS Directive). As per the NIS Directive, Member States were required to provide the Commission with information regarding identification of operators of essential services in their respective jurisdictions until November 9th, 2018. For Belgium, identification of operators in critical sectors such as energy, transport, health and drinking water supply and distribution is pending while Hungary is required to notify about the operators of essential services for the transport sector. Romania's authorities need to provide information on national measures allowing for the identification of operators, the number of operators of essential services and thresholds used in the identification process. The Member States have been given two months to comply with their respective obligations

4.2.2. The Regulation on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification (Cybersecurity Act)

In the recent years, the EU has taken great strides to bolsters its resilience and its capabilities to identify, prevent, deter and respond to cyber-attacks and other malicious activities. The

[176] For example, see also https://www.bbc.com/news/technology-52646808 https://www.bloomberg.com/news/articles/2020-03-23/paris-hospitals-target-of-failed-cyber-attack-authority-says

[177] Cybersecurity in the healthcare sector during COVID-19 pandemic, available at: https://www.enisa.europa.eu/news/enisa-news/cybersecurity-in-the-healthcare-sector-during-covid-19-pandemic

[178] Cybersecurity – review of EU rules on the security of network and information systems, available at: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12475-Revision-of-the-NIS-Directive

[179] Combined Evaluation Roadmap, Revision of the NIS Directive, available at: https://ec.europa.eu/info/law/better-regulation/

[180] Cybersecurity: Commission urges Belgium, Hungary and Romania to comply with their obligations regarding operators of essential services, available at https://ec.europa.eu/digital-single-market/en/news/cybersecurity-commission-urges-belgium-hungary-and-romania-comply-their-obligations-regarding

enactment of the Regulation on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification[181] (CSA) in 2019 was one such initiative by the Commission to strengthen the EU Agency for cybersecurity (ENISA) and to create an EU-wide cybersecurity certification framework for digital products, services and processes.

While the enactment of the CSA granted ENISA a permanent mandate along with more resources and tasks, the disruption caused by the COVID-19 pandemic put the agency's capacity-building and preparedness capabilities to the test. As the situation with the pandemic continued to escalate, ENISA launched a dedicate webpage that provided resources and publications on cyber safety tips and measures that can be taken by organisations, businesses as well as citizens. [182] In addition, ENISA also released a series of publications in October 2020 highlighting the threat landscape pertaining to different challenges including spam, data breaches, malware, phishing and crypto jacking.

Notably, the European Cloud Service Provider Certification (CSPCERT) Working Group, a private and public stakeholder group, was created to explore the possibility of establishing an EU-wide framework for cybersecurity certification of ICT services, products and processes as provided for under the CSA. In June 2019, the CSPCERT published a set of recommendations in relation to the security certification of cloud services to ENISA, the European Commission and the Member States.

Pursuant to the CSA, ENISA also launched a month-long public consultation in July 2020 for the first candidate cybersecurity certification scheme, the Common Criteria based European cybersecurity certification scheme (EUCC). The EUCC scheme will replace the existing Senior Officials Group Information Systems Security Mutual Recognition Agreement (SOG-IS MRA) and extend the scope so as to cover all EU Member States. To assist with this transition as well to ensure consistent application of the CSA, the European Cybersecurity Certification Group (ECCG) was established. The ECCG comprises of representatives of national cybersecurity certification authorities or the representatives of other relevant national authorities. ENISA has also set up a 15-member working group on Cybersecurity for Artificial Intelligence to advise ENISA on matters and developments relating to AI cybersecurity and to support ENISA in creating risk-proportionate cybersecurity guidelines for AI.

4.2.3. General Data Protection Regulation

25 May 2020 marked the second anniversary of the application of Europe's Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data[183] (GDPR) which, as discussed in D4.1, was enacted to harmonise and strengthen the fundamental rights of individuals pertaining to processing of personal data. The Communication published by the European Commission regarding the evaluation of the GDPR took into account input from the European Parliament, the

[181] 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) OJ L 151
[182] ENISA, COVID19 webpage, available at: https://www.enisa.europa.eu/topics/wfh-covid19?tab=details
[183] 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

European Data Protection Board, individual data protection authorities and other stakeholders. [184] As per the said report, the general view was that the GDPR was able to successfully achieve the objectives of strengthening individuals' right to personal data protection as well as guaranteeing free flow of personal data within the EU, however, areas for future improvement were also identified.

The Communication highlights that while the GDPR provides for a consistent approach pertaining to data protection in the EU, it does give Member States discretion in certain areas. This has resulted in diverging approaches and fragmentation that has subsequently created challenges to conducting cross border business, innovation, in particular as regards new technological developments and cybersecurity solutions.[185] As a part of its action items necessary to support the application of the GDPR, which is relevant for the purpose of this deliverable, the Commission has stated that it will support standardisation/certification in particular on cybersecurity aspects through the cooperation between the European Union Agency for Cybersecurity (ENISA), the data protection authorities and the European Data Protection Board.

As per the Commission, the COVID-19 pandemic underscored the flexibility provided by the GDPR, especially in relation to the design of contact tracing apps and other innovative solutions to combat the pandemic. [186] As the pandemic escalated, Member States were scrambling to build effective contact tracing apps that would alert its users whenever they came in contact with someone who had tested positive for the coronavirus. However, given that the coronavirus does not stop at borders, a need was felt to devise an interoperability solution for national contact tracing apps to allow citizens to get the relevant information from one single app while travelling in Europe. In this context, the European Data Protection Board issued a statement on the data protection impact of the interoperability of contact tracing apps. The information security aspect was highlighted as a key issue that had to be taken into account by providers of contact tracing apps including security of data in transit for the possible interconnection of back-end servers.[187]

The pandemic also required processing of health data on a large scale by hospitals, public authorities, employers and the like. Article 9 of the GDPR deals with processing of special categories of data which includes biometric data, data concerning health, genetic data, data revealing racial or ethnic origin, political opinions and religious or philosophical beliefs. Given the nature of such data, Article 9 of the GDPR prohibits its processing unless conditions under Article 9(2) are met.

It is pertinent to note that the Statement by the European Data Protection Board (EDPB) acknowledged that the GDPR already contains provisions allowing competent public authorities as well as employers to process personal data in the context of an epidemic provided that it is done in accordance with national law and within the conditions set

[184] Communication from the Commission to the European Parliament and the Council, Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0264

[185] It should be noted that on 16 July 2020, the Court of Justice of the European Union invalidated the EU-US Privacy Shield, the framework that enabled data transfers between the EU and the US. However, the landmark decision is not directly relevant to the scope of this deliverable.

[186] It should be noted that on 16 July 2020, the Court of Justice of the European Union invalidated the EU-US Privacy Shield, the framework that enabled data transfers between the EU and the US. However, the landmark decision is not directly relevant to the scope of this deliverable.

[187] European Data Protection Board, Statement on the data protection impact of the interoperability of contact tracing apps, available at: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_statementinteroperabilitycontacttracingapps_en_0.pdf

therein.[188] Article 6 and 9 of the GDPR enable processing of personal data including special categories of data by competent public authorities such as public health authorities. In the context of employment, the EDPB Statement clarified that processing of personal data may be needed to comply with legal obligations to which the employer is subject such as obligations relating to health and safety in the workplace, or to the public interest, such as the control of diseases and other threats to health.[189]

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

Given the ever-increasing value of data and the value that it can add to existing services and business models, the Regulation on a framework for the free flow of non-personal data in the European Union[190] was enacted to remove obstacles to the free movement of data. Member States have time until 30 May 2021 to repeal any existing data localisation requirement that is laid down in a law, regulation or administrative provision of a general nature.

In order to achieve the objectives envisioned in Article 6 of the Regulation, the European Commission established the multi-stakeholder group, SWIPO (Switching Cloud Providers and Porting Data). Article 6, which deals with porting of data, requires the European Commission to encourage and facilitate the creation of self-regulatory codes of conduct at Union level so as to contribute to a competitive data economy. After more than two years of work, SWIPO published the Codes of Conduct for Infrastructure as a Service (IaaS)[191] and Software as a Service (SaaS)[192] in July 2020. The Codes provide guidance to cloud providers as well as cloud customers on safe and effective switching of cloud providers and porting of non-personal data. By helping cloud customers understand the relevant processes that are involved for the transfer of data, the Codes help prevent "vendor lock-in." The Codes also require cloud providers to provide a transparency statement that will enable customers to gauge how the provider will support the switching process and facilitate safe transfer of data to the new cloud provider.

4.2.5. Product Liability Directive

Unlike the GDPR which completed merely 2 years of application, the Directive concerning liability for defective products[193] (PLD) turned 35 in 2020. Since its enactment, the PLD

[188] European Data Protection Board, Statement on the processing of personal data in the context of the COVID-19 outbreak, available at: https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[189] European Data Protection Board, Statement on the processing of personal data in the context of the COVID-19 outbreak, available at: https://edpb.europa.eu/sites/edpb/files/files/news/edpb_statement_2020_processingpersonaldataandcovid-19_en.pdf

[190] 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

[191] Code of Conduct for Data Portability and Cloud Service Switching for Infrastructure as a Service (IaaS) Cloud service, available at: https://swipo.eu/wp-content/uploads/2020/10/SWIPO-IaaS-Code-of-Conduct-version-2020-27-May-2020-v3.0.pdf

[192] Switching and Portability of data related to Software as a Service (SaaS), available at: https://swipo.eu/wp-content/uploads/2020/07/SWIPO-SaaS-Code-of-Conduct.pdf

[193] Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products OJ L 210

ensured a high level of consumer safety and protection and held producers liable for any damage that resulted from the use of their defective products. As highlighted in D4.1, the Commission had launched a public consultation in 2017 to assess the relevance of the PLD in the context of new technologies. Subsequently the Commission published the Fifth Report on the application of the PLD in May 2018 wherein it acknowledged that the effectiveness of the PLD was hampered by concepts such as 'product', 'producer', 'defect' or 'damage' which could be more effective in practice.[194] The report highlighted additional aspects that needed to be looked into while stating the aim of the Commission to put in place a positive and reliable framework for product liability that fosters innovation, jobs and growth while protecting consumers and the safety of the general public.[195]

Since the publishing of D4.1 in December 2019, many initiatives have been taken at an EU level regarding existing framework pertinent to product liability. In February 2020, the Committee on the Internal Market and Consumer Protection passed a motion for resolution wherein it called on the Commission to review the PLD along concepts such as 'product' 'damage' and 'defect' and to make proposals to update these concepts and rules if necessary. The Report by the Expert Group on Liability and New Technologies rightly notes, "With enhanced complexity, openness and vulnerability, there comes a greater need to introduce new safety rules. Digital product safety differs from product safety in traditional terms in a number of ways, including by taking into account any effect a product may have on the user's digital environment. Even more importantly, cybersecurity has become essential."[196] At a national level, Member States have been discussing various options for modifying their national rules in line with the challenges presented by new technologies.[197]

4.2.6. Radio Equipment Directive

The Directive on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment[198] (RED) provides a framework for placing radio equipment on the market. 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 radiodetermination, or electrical or electronic products which must be completed with an accessory, such as antenna, so as to intentionally emit and/or receive radio waves for the purpose of radio communication and/or radiodetermination.[199] The RED provides a framework to ensure that such products meet certain standards for various aspects including safety, health and electromagnetic compatibility.

---

[194] 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), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:246:FIN

[195] The European Consumer Organisation, Product Liability 2.0 : How to make EU rules fit for consumers in the digital age, available at: https://www.beuc.eu/publications/beuc-x-2020-024_product_liability_position_paper.pdf

[196] Expert Group on Liability and New Technologies - New Technologies Formation, Liability for Artificial Intelligence and other emerging digital technologies, available at: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=63199

[197] The European Consumer Organisation, Product Liability 2.0 : How to make EU rules fit for consumers in the digital age, available at: https://www.beuc.eu/publications/beuc-x-2020-024_product_liability_position_paper.pdf

[198] 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

[199] 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).

Article 3(3)(e) and (f) of the RED require radio equipment within certain categories or classes to incorporate safeguards to ensure that the personal data and privacy of the user and of the subscriber are protected and to support certain features ensuring protection from fraud respectively. An impact assessment study was conducted on behalf of the Commission between April 2019 and March 2020 to analyse the different policy options to strengthen safeguards for internet-connected radio equipment (RE) and wearable RE as regards data protection and privacy and protection from fraud and to verify whether a minimum level of "baseline" security requirements measures should be integrated into the RED.[200] The study involved assessment of relevant EU legislation, more than 70 interviews with relevant stakeholders and two online surveys. Based on this process, the study provided recommendations which included adoption of two delegated acts based on Articles 3(3)(e) and 3(3)(f) which would strengthen the RED's essential requirements to close regulatory loopholes. The study also recommends bringing all internet-connected radio equipment within the scope of the RED to strengthen security in respect of data protection and privacy and protection from fraud.[201]

With respect to Article 3(3)(i), the RED requires radio equipment to support certain features in order to ensure that software can only be loaded into the radio equipment where the compliance of the combination of the radio equipment and software has been demonstrated. Similarly, Article 4 of the RED requires manufacturers of radio equipment and of software allowing radio equipment to be used as intended to provide Member States and the Commission with information on the compliance of intended combinations of radio equipment and software with the essential requirements set out in the RED. To better understand the different aspects relating to the upload of software into specific categories of devices governed by the RED, the European Commission launched a targeted consultation as well as a public consultation in February and May 2020, respectively. The consultations also aimed at gleaning input regarding legislative options that would ensure that equipment classes remain compliant when new software is uploaded.

4.2.7. Regulation on Electronic Identification and Trust Services

A 2020 survey that interviewed approximately 27,500 people from 28 Member States revealed that a large majority would consider it useful to have a secure single digital ID that could serve for all online services while also giving them control over the use of their data. [202] Secure and trusted electronic transactions are essential for the EUs internal market, especially at a time where the COVID-19 pandemic has seen more governments and organisations move their services and operations online. The Regulation on electronic identification and trust services for electronic transactions in the internal market[203] plays a fundamental role in this area by providing an advanced legal framework for cross-border electronic identification, authentication and website certification within the EU. Additional information on the services provided by the eIDAS Regulation can be found in Section 4.1.8 of D4.1.

[200] Impact Assessment on Increased Protection of Internet-Connected Radio Equipment and Wearable Radio Equipment, available at: https://ec.europa.eu/docsroom/documents/40763/attachments/1/translations/en/renditions/native

[201] Inception Impact Assessment, Revision of the eIDAS Regulation – European Digital Identity (EUid), available at: https://ec.europa.eu/info/law/better-regulation/

[202] Special Eurobarometer 503, Attitudes towards the impact of digitalisation on daily lives, available at: https://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/89800

[203] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257

In July 2020, the European Commission launched a public consultation to gauge the drivers and barriers to the provision of electronic identification and trust services for electronic transactions in the EU. The Inception Impact Assessment (IIA) report published along with the consultation highlights various problem areas that need to be tackled. For instance, only 15 of 27 Member States offer cross-border electronic ID under eIDAS to their citizens.[204] The IIA also highlights that while solutions offered by social platforms provide convenience, they are disconnected from an authenticated physical identity which makes fraud and other cybersecurity threats difficult to manage.[205] The overall assessment will also take into account the developments in the technological and policy area, such as the escalating reliance on doing business online. In March 2020, the Connecting Europe Facility launched the 2020 CEF Telecom eIdentification & eSignature call for proposals in the domain of eIdentification and eSignature. [206]

4.3 Update on the Upcoming Regulatory Landscape

This section provides an overview of the most relevant -possibly- upcoming EU regulations that are related to the project's scope. At the moment of the drafting of the present document, these regulations are found at a proposal stage and, they are, therefore, not applicable. Despite the fact, though, that 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 Regulator, including, this of the endorsement of a "data centric" approach, put forward by the European Commission earlier this year[207].

4.3.1. The Data Governance Act

On 25th November 2020, European Commission published a Proposal for a Regulation on European data governance (Data Governance Act)[208]. The overarching objective of the proposal is to strengthen availability of data for use by increasing trust in data intermediaries and by strengthening data-sharing mechanisms across the EU.

To this end, the proposed Regulation introduces a number of measures to increase trust in data sharing, creates new EU rules on neutrality to reinforce the role of data intermediaries in relation to data sharing and provides for measures to facilitate the reuse of certain data held by the public sector. Moreover, the proposal facilitates companies and individuals to voluntarily make their data available for the wider common good under specific conditions.

[204] Inception Impact Assessment, Revision of the eIDAS Regulation – European Digital Identity (EUid), available at: https://ec.europa.eu/info/law/better-regulation/

[205] Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1537349553647&uri=CELEX:52018PC0630

[206] Call for proposals concerning projects of common interest under the connecting Europe facility in the field of trans-European telecommunication networks, available at: https://ec.europa.eu/inea/sites/inea/files/cefpub/2020-1_eid_esignature_call_text.pdf

[207] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European strategy for data, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0066&from=EN

[208] 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

In this context, it can be argued that the earlier stated proposal will probably incentivize data sharing -especially- in the public sector, thus, fostering a culture, which may encourage, also, threat intelligence sharing, particularly relevant for the scope of CONCORDIA.

4.3.2. Regulation for European Cybersecurity Competence Centre

The proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres [209] (Regulation) is especially of relevance to project CONCORDIA given the similarities in objectives set out in the Regulation as well as CONCORDIA. The proposal for the Regulation was presented by the Commission in September 2018 to secure its Digital Single Market by enabling the EU to retain and develop the requisite cybersecurity technological and industrial capacities. The proposal focuses on creating a network of national coordination centres, a European Cybersecurity Industrial, Technology and Research Competence Centre and a Cybersecurity Competence Community.

While Trialogue negotiations regarding the proposal for the Regulation had started in March 2019, no additional action was taken due to the short timeframe.[210] At the time of publishing D4.1, the status of the Regulation remain unchanged. On 19 October 2020, the proposal for the Regulation was included as one of the "priority pending proposals" in the Commission Work Programme 2021 (Annex III). [211]

On 11th December 2020, EU institutions reached a political agreement on the Cybersecurity Competence Centre and Network, an initiative that strives to enhance and fortify technology and industrial cybersecurity capacities in the EU and to help create a safe online environment.[212] The Cybersecurity Competence, which will be situated in Bucharest, along with the Network of National Coordination Centres will work in tandem to bolster cybersecurity capabilities, safeguard the EU from cyber attacks and reinforce the competitiveness of the EU industry in the said field. The agreement, however, is subject to formal approval by the European Parliament and the Council of the EU which is expected to take place in January 2021.

4.3.3. ePrivacy Regulation

The Commission's proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications (ePrivacy Regulation) in January

[209] Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1537349553647&uri=CELEX:52018PC0630

[210] Legislative Train, Proposal for a Regulation establishing the European Cybersecurity Industrial, Technology and research competence centre, available at: https://www.europarl.europa.eu/legislative-train/api/stages/report/current/theme/connected-digital-single-market/file/european-cybersecurity-competence-centers

[211] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Commission Work Programme 2021, available at: https://ec.europa.eu/info/sites/info/files/2021_commission_work_programme_annexes_en.pdf

[212] Press Release, Commission welcomes political agreement on the Cybersecurity Competence Centre and Network, available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_20_2384/IP_20_2384_EN.pdf

2017 aimed at correcting the inconsistencies and fragmentation that resulted from the different approaches taken Member States while transposing the Directive on Privacy and Electronic Communications (ePrivacy Directive) into their national laws. While the Commission aimed at implementing the ePrivacy Regulation along with the GDPR, consensus from other Member States has not been achieved despite numerous revisions to the original proposal for the ePrivacy Regulation. At the time of drafting this deliverable, the Presidency of the Council of the European Union released the latest draft of the proposal[213], however, there is no given timeline on when the ePrivacy Regulation will be approved and enacted.

4.4 Implementing Cybersecurity Principles: The Interview Series 2020

4.4.1. From Why to How

In the past decade, the discussion about the 'why' of cybersecurity and related non-functionals such as data protection, privacy, e-privacy and cyber-physical safety has finally been settled. All stakeholders, including society, agree that cybersecurity is a need-to-have.

This leads us to the 'how'. How to implement cybersecurity, safety & privacy principles in practice; all the way up stream by design as well as further and all the way downstream, including both the organizational aspects and preconditions of implementing.

In 2020, CONCORDIA started an initial series of qualitative interviews about the 'how', with experts from the practical and otherwise operational side. The already conducted interviews were with Consortium partners, representing industry.[214] In 2021 it is anticipated that also other partners representing industry and academia, as well as other members of the CONCORDIA ecosystem both at national and European level will be interviewed in the same manner. The novel element about these interviews is that these are not conducted with legal or policy persons as interviewees, but instead let the 'market' speak up, with a principles-based approach that, for instance with open queries such as:

A. How are you and your organisation currently considering and implementing cybersecurity and related principles? How would you like to do it or see it done?

[213] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_9931_2020_INIT&from=EN

[214] For the related considerations pertinent to the gaps and recommendations in the public sector, there are two publications where the results from the nationwide survey, conducted in Greece in 2019, were discussed. For more information see also "Cybersecurity Assessment of the Public Sector in Greece", Drivas, George; Maglaras, Leandros; Janicke, Helge; Ioannidis, Sotiris, European Conference on Cyber Warfare and Security, 2019 Portugal and "Assessing cyber security threats and risks in the public sector of Greece", G. Drivas, L. Maglaras, H Janicke, S Ioannidis, Journal of Information Warfare. Both publications elaborate on the findings of the survey conducted in the public sector, focused on determining the cybersecurity posture of public entities and concluding with proposals about the future path. In 2020, a new survey has not been conducted, since the findings of the 2019 survey are considered still valid.

B. What are your thoughts and suggestions about the proposed European Cybersecurity Competence Center structure[215] (which is part of the European Cyber Strategy[216]) and envisioned challenges and benefits?

4.4.2. Principles-based Approach

The principles-based approach has been chosen as in this Digital Age we have moved from stand-alone to connected, interconnected and hyperconnected systems. We have moved from silo-ed and static to a dynamic and converging world, both in cyber, cyber-physical as well as cross-cutting though and interconnecting sectors and markets through the European Union and beyond. Furthermore, malicious actors change their ways as soon as their existing ways have been blocked; thinking and acting dynamic, in a continuous, iterative and evolutionary way, is the only way to cope with cybersecurity, safety, data protection and the like. And, last but not least, at least since 2016 the European Union has issued current and is developing and issuing upcoming legislation and other policy instruments that are principle-based as well, providing sectors, society, digital ecosystems and other markets in this Digital Age with principle-based frameworks. These need to be loaded, and with the principles-based approach this can be done in a practical way; risk- and impact-based, human-centric, data-centric, lean, agile, with room to manoeuvre, dynamically assured, and therefore future-proof. The principles-based approach therefore is a prerequisite to help loading those frameworks, towards a digital single market, and digital sovereignty.

In an open dialogue (under Chatham House Rule) initially the flow of the conversation was the 'State of Play': 'Where are we today?', thereafter the 'State of the Art': 'Where should we go', and then of course the GAP thereof: 'How to bridge the GAP, how to get there, and what does it take?'. Based on your inputs, we will further document the related gap analysis between the current State of Play and the State of the Art, as visualised in Figure 3 below.

Figure 3: Gap analysis between the current State of Play and the State of the Art based on input from Consortium Partners

[215] Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1537349553647&uri=CELEX:52018PC0630

[216] EU Security Union Strategy, including an overview of all relevant initiatives: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1596452256370&uri=CELEX%3A52020DC0605

4.4.3. Common Denominators in the Interviews

A common denominator that has been perceived during the interviews conducted up to the date of the edition of this deliverable is the fact that no sector (neither public nor private), no market and no society or economy is safe from cyber-attacks, so it is even more important that legislation and other clear policy instruments help, incentivises and obligate to operationalise and implement cybersecurity, safety and privacy principles in all relevant domains and dimensions.

Another common denominator identified is that it is crucial to establish mechanisms 'by design by default' measures – both technical and organisational – and other mechanisms for appropriate levels of cybersecurity, safety, data protection, resilience, dynamic certification and assurance, and digital sovereignty measures.

It was also generally identified that one of the main challenges is how to introduce and implement general security-principles and generic cybersecurity controls and measures in horizontal regulations (such as the Cybersecurity Act (CSA) but also, Radio Equipment Directive (RED), General Data Protection Regulation (GDPR), General Product Safety Directive (GPSD), Machinery Directive, NIS Directive, eIDAS Regulation (EUid), Sales of Goods Regulations and the like). Moreover, this has to be done while avoiding overlap or at least avoiding conflicts between specific vertical regulations (such as for instance the Medical Device Regulation (MDR), regulatory standards such as the RTS of the Second Payment Services Directive 2 (PSD2) and many others).This will result in delays in implementation and enforcement capabilities, as well as delay in building and achieving digital sovereignty – in the respective sectors, markets and between respective stakeholders on what applies, prevails, how to address conflicts, who is allowed to enforce what, et cetera.

4.4.4. Implementing Cybersecurity Principles, from an Aerospace Sector perspective

The aerospace sector is used to being highly aware of and fully engaged with functional safety of any kind. Implementing safety measures are expensive, especially in this sector as per certification requirements; unsafety however is much more expensive. That security is safety, is a given in the sector.

Also, from safety and security perspective aircrafts are seen as systems. Even more so, these systems generally have a lifetime of at least 20 to 30 years. Having a system life cycle approach is thereof a prerequisite. As the aerospace sector is used to this, other sectors can learn a lot from its good practices and lessons learned.

In aviation, strict protocols must always be followed. Any change must be verified in the certification process. Regarding cybersecurity, one of the challenges is air traffic communication, which has been – intentionally – unencrypted since the 1960s and can be intercepted very easily. Another major challenge is that although aircrafts are subject to a very rigid certification process, the challenges in this Digital Age including cybersecurity threats and related consequences are generally not addressed, yet. Therefore, in the near future, it would be necessary to include cybersecurity capabilities in aviation certification procedures and to upgrade certification procedures in this area as well.

Another main challenge from the designer's point of view is that they do not have clear requirements that can guide them in the way other requirements are known to them and

implemented. This is especially critical as per the lifetime of the systems and their respective life cycles. At this moment, there is still a substantive gap between technology, regulations, and the actual situation, this also as the evolution in aircraft design is a very slow process. And this poses security challenges. If one changes something in an aircraft, there is a strict certification process. This is not always beneficial to security, as one is not allowed to change anything without certification. Some shifts have taken place with the draft of a new aerospace regulation in 2010 which involves manufacturing in the process; however, this regulation is still not in force. In order to change the situation accordingly, it would be crucial to introduce a life cycle approach and change the certification system accordingly.

In the coming years rapid development is expected in autonomous aircrafts, drones, other (un)manned aerial vehicles, either piloted remotely or otherwise. Currently they do not fly autonomously, although there are some automated processes, for instance for landing. Especially while developing towards full autonomy, all aspects of safety, security and data protection must be considered at the development stage, while ensuring compliance with the legislation. For instance, uncontrolled recording can significantly interfere with the privacy and other rights of persons, so these aspects must be considered already in the development phase and implemented in a way that adequately protects the rights of individuals and is compliant with GDPR and other regulations.

One of the considerations to address part of these challenges is to introduce automated security and privacy incident reports. Furthermore, it is **recommended to work on minimum baseline security and privacy requirements** – with contextual risk- and impact-based measures added where appropriate – for easy and consistent implementation. Another recommendation is to **keep the human in the loop**, and aware, and to build, achieve and sustain a culture that security is as much important as safety, and also security cannot be bolted on in retrospect.

4.4.5. Implementing Cybersecurity Principles, from a Telecom Sector perspective

While the telecom sector has been one of the most experienced sectors in secure communications and demonstrating implementing and continuous mitigation measures regarding security, privacy and the like, some main challenges in this Digital Age when engaging with customers are (i) leakage of personal data – also in view of e-privacy –, and the level of allowance of characterisation of online user behaviour on social media and streaming services.

This obviously includes the re-use of (personal) data obtained by the company based on a legal ground under the GDPR or ePrivacy Directive. This is particularly relevant in this sector where a lot of meta-data is processed, but it also reveals some data about the user. Therefore, it is a great challenge how to ensure that, in accordance with the requirements of the GDPR, the appropriate legal ground (and where not identified, the 'final resort' legal ground of unambiguous informed consent) is assured and will therefore be aware of which data will be processed and in some cases be re-used. Thus, it is a great challenge how to properly explain the content of consent in such a way that the individual understands and is aware what data is concerned, how the data is structured (for instance unaltered, combined or as a pseudonymized zero-knowledge proof attribute), and to what data processing the consent is given. Various technical and organisational measures could facilitate this, for instance by means **improved readability** – both human- and machine-readable – of privacy statements, acceptable use policies or terms of service, contextual consent configurators, consent management custodian, and other data management and accountability tooling.

Whereas some of the collected data reveal the behaviour of an individual very accurately, it would make sense to develop a model by design by default that would not reveal data that could lead to the identification of the individual. In any case, the possibilities of transmitting the collected data to other organisations must be very carefully controlled and, of course, cyber-attacks must be prevented, and the security of the data already collected and otherwise processed must be ensured.

These above-mentioned challenges are amplified because of cloud computing and 5G capabilities and consequences; unification of practically implementable and enforced regulations, standards and protocols at European Union level is crucial, especially in terms of security, privacy, data management and digital sovereignty.

An interesting area that needs to be analysed from the mentioned aspects is also the area of critical infrastructure (finance sector, health care, mobile network, etc.) and automatic software upgrades. During the ongoing global COVID-19 pandemic it has become clear how critical infrastructures, vital systems, essential services but also citizens in their various persona are exposed to cyber-attacks. Therefore, special attention must be paid hereto, while at the same time meeting the conditions for protecting the privacy and rights of individual. **Principle-based, risk- and impact based, human-centric continuous assurance** must be implemented also related to regulatory requirements for ensuring security of critical infrastructures, such as security patching of software. Also, here**, life cycle management of the relevant (eco)systems** is prerequisite.

4.4.6. Implementing Cybersecurity Principles, from a Threat Intelligence perspective

Threat intelligence is not about data. Threat intelligence is about what you do with the data. Threat intelligence is about making informed decisions. All this in an accountable way, meaning with the ability to justify (and where necessary: defend) those decisions.

When we consider the issue of threat intelligence, it is in practice common to limit the distribution of information to the need-to-know principle. Of course, each stakeholder wants to gain as much information as possible, so it is crucial to establish mutual trust and collaborative approach.

Having access to threat intelligence is one thing. Organisations generally consists of various department and units. For instance, corporates could consist of several companies that specialize in different areas of operation. A big organisational challenge is the transfer of data internally, as each has different roles and responsibilities, and some of which operate cross-sectors. This requires coordination, understanding, trust and management, which generally is not yet sufficiently in place.

Each organisation must consider in its internal structure how technology and requirements for safe and legal operations will be integrated. In order to achieve the set goals, it is necessary to set priorities. The latter requires effort, budget and understanding the various interests. Despite the awareness of how important it is to ensure security; threat intelligence is still not a priority in some places and organisations – both in the public and private sector – generally deal with it spontaneously, ad hoc and at forensic levels.

It is therefore essential to put in place and implement mechanisms to help **bridge the gaps, ensure the objectives set, find common grounds, align goals with hybrid governance models and controls,** and focus on preventative and other upstream and midstream measures and capabilities. With those, trusted intelligence and other data sharing should not be that big of a problem.

4.4.7. Implementing Cybersecurity Principles, from a Research Institute Sector perspective

Focussing on how to certify and otherwise assure digital products, systems and services, on the main challenges is the fragmentation of the certification domain. Where standards such as the ISO 27000 series focus on certain security controls, they provide certain level of security for a particular process. However, these do not provide the appropriate level of security – or level of trust in general – of whole sets of products, systems and services, where every single component is important yet interconnected and not isolated. So, a more systematic approach is required.

When assessing digital ecosystem, certain technical layers, or organisational dimensions (such as data, identity and human dimensions) can be identified as not yet well-addressed enough. For instance, there is hardly any certification of software.

A more dynamic approach is required as well. Regulatory requirements related to for instance personal data processing (article 25 GDPR) or personal data protection (article 32 GDPR), which are data-centric and dynamic, are deemed to be very tricky to implement from a technical perspective. This, also as the GDPR is purpose-centric, where in the real-life multiple purposes can be pursued with the same product, system or service.

For the current generation of engineers, the qualitative approach and related principle-based implementations are still difficult to grasp, as generally quantitative and rule-based implementations are better known and within the current comfort zone.

Therefore, **the testing of (end-to-end eco-) systems and services** is becoming much more important, and essential. Merely assuring a document or verbal information to verify compliance to a standard, which is generally still the current practice, is clearly insufficient. Think for instance about IoT ecosystems. This is one of the reasons why CONCORDIA is focussing a lot on cyberranges and related virtualised ecosystems. With that, near-real time continuous monitoring and dynamic assurance have come a bit closer to reality.

4.4.8. Implementing Cybersecurity Principles, from the eHealth Sector perspective

Implementation of cybersecurity principles are not necessarily difficult. However, their implementation depends on whether a component or relatively low-risk low-impact device is the subject matter. Furthermore, their implementation depends on whether it concerns end-to-end, IoT or other connected, interconnected or hyperconnected systems involving, for instance, sensitive data processing. In the health sector most, personal data is generally sensitive data, which is a special category of data under the GDPR.

One of the main challenges is that there are different regulations, standards and good practices where each member state seems to have a different priority. This leads to

fragmentation and does not cater to the mission of a digital single market or digital sovereignty. On the latter, the COVID-19 pandemic has tested the capabilities and endurance primarily of the national healthcare systems, both from public sector as from private sector perspective; these have been stretched to the limit in handing this extraordinary pandemic and remain vulnerable to phishing, data breaches, social engineering, cybersecurity attacks, and regulatory non-compliance. It also has shown that coordination and collaboration between the public sector and private sector, and vice versa are a prerequisite.

An additional main challenge is to make individuals and organisations aware and appreciative about the various personas an individual has (such as consumers, professionals, civil servant, patient, non-patient, and the like) and what that means in the domain of cybersecurity, (personal) data protection, data management and resilience. It is seen as one of the starting points towards digital sovereignty as well.

Alignment and harmonisation of security measures and cybersecurity schemes are other essentials to bridge the GAP, and for some European sectors it is a must-have. Healthcare is seen as such high priority sector, also as it is within scope of the NIS Directive – although not all member states have taken that in, to various extents –.

In the healthcare sector, same as in the aerospace sector as mentioned above, certification processes are lengthy and static processes that do not cater for the challenges and opportunities of this Digital Age. One of the recommendations to bridge the GAP is to **discuss and establish what can be certified**, what not, and how to assure anything that cannot (yet). Think for instance about e-health products, systems and services that have a certain level of complexity while also have a relatively long lifetime. **Providing guidance on all phases of the value chains can provide the trust that manufacturers, integrators, vendors, service providers, customers and consumers need**. In the short term and midterm focussing on such guidance in particular phases of the value chain can already boost such trust, while developing and implementing others in the remaining parts of the value chain. Having a silo-ed approach will not help, and further increase unwanted fragmentation.

4.4.9. Implementing Cybersecurity Principles, from the Financial Industry Sector perspective

The digital transformation of the financial industry sector is still ongoing. One of the main challenges that each financial institution is responsible for is its own compliance, and digital transformation capabilities such as cloud computing and related compliance issues not yet grasped to the full. A few of those are the level of control, level of dependence, and level of digital sovereignty such financial sector (and its customers) has when outsourcing computing, data processing and the like, and in how and to what extent it can continuously monitor and satisfactorily prove that to the relevant authorities.

However, on cybersecurity, increased phishing and social engineering are deemed to be the major challenge. For that, improvement in the field of digital identity can surely add to bridging the GAP. This, also as per the increased remote communication and engagement in society in general – expedited and otherwise increased by the COVID-19 pandemic – and between financial institutions and their customers in particular. Except for the eIDAS Directive and current review thereof (towards the expected eIDAS Regulation (EUid)),

digital identity is a vast domain that needs to be catered for, but most of all needs and deserves implementations. Technically and organisationally, this is possible, also in a GDPR-compliant way, but no real uptake has been seen yet, even while it as expected that the PSD2 Directive would have incentivised this. This also, as these digital identity platforms and related schemes need a certain scale, and currently it is too much silo-ed and fragmentated per Member state, and per bank or per other financial institution. Another reason is that human behaviour still is always easy to predict and cater for.

Two ways of support bridging the GAP is to both assess, **map and plot the numerous and various personas and characteristics of individuals and related user experiences (UX),** and **to coordinate and orchestrate** (the implementation of) **a truly European, human-centric, interoperable, agile and trustworthy digital identity ecosystem of ecosystems.**

From the financial industry sector perspective, being granted trust as well as the appropriate room to trial and test – at scale – across Member states and sectors, so for instance in European living labs and other sandboxes, is seen as highly recommended to give the market the ability to accelerate European innovation, to cater for rapid innovation and continuous improvement in this dynamic Digital Age.

4.4.10. Key Takeaways & Recommendations

Based on the earlier discussion captured -especially- under section 4.4, this section summarizes the emerging key findings and the resulting early-stage recommendations.

- Fostering accountability by identifying responsibilities

No organisation is immune to cyberattacks and can have a major impact on the financial position, market goodwill and consumer trust. Hence, as opposed to taking a reactive approach wherein organisation take charge "after" an incident has taken place, being proactive by assigning tasks and duties to individuals within the organisation can go a long way in securing an organisation. Accountability is an enabler as it helps individuals understand their role in the security context and in the event of an untoward incident and equips them with the necessary skills to mitigate the impact.

Identifying responsibilities would also include involving audit teams, whether internal or external, to assess the effectiveness of the cybersecurity controls. Doing so can help organisations identify and strategically prioritise the cybersecurity threats by leveraging on the expertise of such teams. Moreover, such teams can help organisations design effective controls and processes to address identified threats. External audits can be more beneficial as they bring a fresh set of eyes to evaluate processes, controls, and areas that carry the highest risk of fraud or error.

- Technical measures

The GDPR requires organisations that are processing personal data of EU residents to ensure that it has implemented appropriate technical measures to ensure a level of security appropriate to the risk.[217] This would entail the use of firewalls, anti-spam, anti-virus, and

217 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

intrusion detection systems (IDS) systems that can act as gatekeepers and prevent unauthorised parties from gaining access to the systems of an organisation. Moreover, it is imperative that these tools are regularly updated to ensure their effectiveness. Strong authentication is also one of the many pillars to ensure a fortified cybersecurity strategy. It ensures that only authorised personnel are able to access the confidential information of the organisation.

Data encryption and pseudonymisation are also measures that can significantly enhance security within the organisation. Data encryption involves conversion of data from a readable format into an encoded format that can only be accessed or decrypted by a user with the correct encryption key. Hence, access to information is limited to those authorised personnel only. Moreover, while encryption does not prevent cyberthreats, it can limit the resulting risk by preventing cyber attackers from decrypting and accessing the data. It is important for organisations to continuously update their encryption algorithms as older ones can be easier for hackers to decipher.

On the other hand, pseudonymisation refers to the process of de-associating a person's identity from the personal data being processed by replacing one or more personal identifiers, i.e. pieces of information that can allow identification (such as e.g. name, email address, social security number, etc.), relating to the said with the so-called pseudonyms, such as a randomly generated values.[218] If done properly, pseudonymisation not only can help an organisation enhance the security of personal data as well as support its overall compliance with the GDPR data protection principles.[219]

- Organisational Measures

Within an organisation, it is important to build a culture of security awareness by implementing relevant measures. Depending on the size of the organisation and the nature of its industry, information management and cybersecurity policies should be devised taking into account the different departments of the organisations. Organisations should also formulate Bring-Your-own-Device (BYOD) policies given that the devices used by employees can increase infiltration of malware and other risks. Given that an increasing number of people have been working from home during the COVID-19 pandemic, a Remote Access Policy is a must to ensure security.

Several data breaches that have taken place in the last few years resulted from inadvertent human errors, hence, maintaining a skilled workforce that receives proper and continuous security training is essential. Regular and ongoing training sessions will ensure that they latest information, guidance, legislations and regulations are known and understood

- Continuous Appropriate Dynamic Accountability

As is evident from the discussion in the chapters above, challenges to cybersecurity are not static and the threat landscape is constantly evolving. While companies might invest in bolstering the security of their infrastructure, systems, and processes, it is imperative to

218 ENISA, Recommendations on shaping technology according to GDPR provisions, available at: https://www.aepd.es/sites/default/files/2019-09/recomendations-on-shaping-technology-according-to-GDPR-provisions-1.pdf

219 ENISA, Recommendations on shaping technology according to GDPR provisions, available at: https://www.aepd.es/sites/default/files/2019-09/recomendations-on-shaping-technology-according-to-GDPR-provisions-1.pdf

remember that cybercriminals also adapt their methods accordingly. As per the 2020 ENISA Threat Landscape, cyber-attacks are becoming more sophisticated, targeted, widespread, and undetected. Hence, security measures that are implemented need to be reviewed in a continuous manner to assess their effectiveness in line with the changing environment.

In today's time, for a cybersecurity process to be effective, it is essential that they aim for 'achieving continuous improvement' wherein the ecosystems, products and services in the Digital Age are provided up-to-date levels of protection by requiring the levels of security and protection to continuously meet their respective appropriate levels i.e. Continuous Appropriate Dynamic Accountability (CADA).[220] This would require organisations to maintain situational awareness across the organisation and identify potential threats and risks. Information would have to be collected and analysed on all security controls to identify vulnerabilities that could be exploited by hackers. It's important to note that CADA cannot be achieved by a single department or team of an organisation but requires the active participation and contribution of the workforce as a whole.

- Established information-security management structures

Based on the discussion in the chapters above and a general understanding of how cyberthreats are proliferating, it is evident that preparation is key. This could entail having a dedicated department or team that is responsible for ensuring that sufficient multi-layered processes, measures and safeguards have been implemented based on the dynamics of the organisations. It is imperative that the said team does not work in silos but rather works in tandem with other departments within the organisations to have a broad understanding of potential risks and threats that could impact the organisation.

The same goes for Computer Security Incident Response Teams (CSIRT) on the top organisational layer, therefore working on a national level. A Network of the national Computer Security Incident Response Teams (CSIRTs) is only as effective as sharing of mutually collected intelligence data, their immediate categorisation and publishing.

There is a gap in the collaborative protocols governing how vulnerabilities should be assessed and disclosed. Vulnerability disclosure procedures have been a hot topic for many years, despite the fact that its actual relevance was uncertain. Despite the many discussions, however, a clearly agreed procedure has never been established between the community of security researchers and software companies or organizations.

The same is true for national CERTs. The incident reporting required by the NIS directive will have little effect when there is no precise regulation about how and which incident data must or may be shared. This is currently a severe shortcoming of the NIS implementation.

A comprehensive information-security management structure needs to factor in three essential principles: confidentiality, availability and integrity. Confidentiality entails creating systems that ensure that information of the organisation is not accessed by unauthorised individuals or entities. In many cases, the aspect of confidentiality is more of an after-thought, however, organisations must proactively ensure confidentiality of their processes and systems right from the design phase. Availability would mean that

[220] The GDPR also provides for this aspect under Articles 25 respectively 32.

information should be accessible and usable by an authorised person when needed. Moreover, processes should be in place to prevent loss of data due to hacks or data breaches such as regularly conducting data backups. Integrity requires safeguarding the accuracy and completeness of the information.

4.5. Other Takeaways and Recommendations

Following the earlier discussion captured under Chapter 3 and Chapter 4 focusing, also, on the existing challenges regarding the implementation of cybersecurity principles and how to improve it, based on the perception of the interviewees, this section sets the discussion in a wider context. To this end, this section points at the wider impact that shortcomings linked -also- to the implementation of cybersecurity principles may lead to, it touches upon shortcomings of the regulation and it paves a potential way forward. Note that, to the extent relevant, COVID-19 has been taken into account as well.

4.5.1. Dissemination of disinformation and societal impact

As discussed under Chapter 3, digital platforms are ideally placed to facilitate the dissemination of disinformation and conspiracy theories and act to reinforce existing beliefs within established networks of like-minded people due to their echo chamber effect, their lack of transparency, the ease of circulation of messages and difficulties in tracking sources and verifying claims. In this respect, European Commission, in particular, with respect to COVID-19 has stressed the necessity to protect “our democracies against the menace of disinformation", that is -of course- of direct relevance for the establishment of Europe’s Digital Sovereignty[221].

As already evident today, disinformation and targeted campaigns to change public opinion are already taking place and have shown great success, affecting elections in the US and UK and showing how carefully crafted information can spread on the internet and guide public opinion about the existence of COVID-19 virus. Usually hidden under the conspiracy theory umbrella, such information has the potential to significantly affect our future lives and legitimate efforts to contain global incidents like the COVID-19 outbreak. A high-risk scenario is a further evolvement of “Antivac” or similar movement, directly affecting the timeframe to sufficient coverage of vaccinated individuals to contain the pandemic.

Taking constitutional rights into account, aiming for compulsory vaccination is far from feasible, leaving the alternative of containing the spread of disinformation and deliberate efforts for massive public opinion changes. Social media companies already understand that they must be more vigilant. Further, under the public's pressure, mainstream platforms, such as Facebook and Twitter, are trying to remove content deemed to be against the public interest. But these efforts have limited impact as proponents of misinformation and conspiracy theorists have migrated onto other less scrutinized platforms or used coded phrases and dog-whistle messaging to evade detection. Therefore, outside pressure to platform providers represents insufficient control over massive disinformation and a change of opinion, and regulation seems to be warranted.

[221] For more information, se also https://ec.europa.eu/commission/commissioners/2019-2024/breton/announcements/europe-end-naivety_en

GDPR already regulates automated processing to some degree, but the regulation is geared towards the protection of individuals when such automated processing produces legal effects concerning him or her or similarly significantly affects him or her. GDPR gives a few examples, like an automatic refusal of an online credit application or e-recruiting practices without any human intervention[222]. GDPR further emphasises that such processing relates to 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects.

Considering future trends, current regulation may be too narrow, though it forms a sufficient basis for enhancement. **Making this notion wider in the sense that automated processing should fall under this regulation when it affects the individual's opinion would cover profiling and selection of news and other individually filtered content using a simple additional inclusion.**

Further, using consent as an instrument to allow automated filtering of content would provide individuals a tool to completely turn off filtering or at least have access to content that would otherwise be filtered according to the individual's profile. This would at least give individuals a tool to get unbiased information when forming an opinion. This could even be further enhanced by enforcing clear marking of filtered content with the ability to turn it off immediately, similar to the notion of cookie consent that is nowadays common.

4.5.2. AI Generated content and societal impact

As already emphasized in this document, the widespread adoption of artificial intelligence and machine learning introduces essential risks and challenges, where unfair inferences based on untrustworthy data and poisoned models affect automatic decision processes and autonomous systems. All these breaches require, on one side, technical countermeasures, and, on the other side, the involvement of policy makers to reflect changes in current IT environment in EU laws and legislations.

We are migrating from traditional software systems based on deterministic algorithms to systems where ML models' reason on data to calculate a solution to individual instances of a problem. In this context, the need of verifying the non-functional properties of ML models, such as fairness and privacy, becomes fundamental to provide trustworthy systems and services with certified ML-based behaviour.

While anonymization techniques have been substantially adopted in the past, they are not effective against advanced data inference. Additionally, connecting data to individuals may not even be necessary to change the opinion of a subset of the population. Machine learning is very effective in identifying properties of a population, allowing for widespread "opinion attacks" on a scale. Content providing services may have serious difficulties identifying such attacks and finding their existence may be too late (e.g. after the election).

To further suppress all forms of content creation attacks, AI-generated content should be taken into consideration.

222 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)

One of the possible solutions would be a clear distinction between human and computer-generated content. This could be added to avatars or other form of identifiers of the content author. As long as computer generated content was more popular in chat bots and other forms of interaction, it was mostly trivial for the individual to recognize artificial content. Becoming widespread, it is less likely that individuals will be capable of simply identifying artificially generated content. Having information about this covered deep in the policy documents or privacy information will have scarce effect.

Distinction between human, boolean logic and AI logic may be warranted as they have different basis. Bool logic is predictable, human logic is mostly subjective and AI logic may be guided into intentional subjective results with the intent to drive individual's thoughts in the interest of the AI service provider. This calls for action on the required marking of content source, similar to disinformation dissemination prevention discussed previously.

Considering the fact that artificial content is based on behavioural analytics, it is at least indirectly connected to privacy and personal data. At the end, it is affecting the mind of the individual. Therefore, it is practical to cover this aspect in GDPR or related regulation.

5. Economic Perspective

As the digital dependency of businesses increases, they and their users also become more vulnerable to cyberattacks [50] [51], This fact, inevitably brings the economic aspects of digital dependency and operation in focus . Hence, the demand for tools to support businesses in cybersecurity decisions is increasing [50]. Besides that, security investments are not like other investments because security does not generate profit but prevents possible future loss. The T4.3 investigations have been determining measurable facts to understand cybersecurity from an economic perspective. For that, it is important to develop and promote tools and frameworks that determine a feasible and analytical path for the estimation of impacts of cybersecurity economics and that supports the simplification process essential for wide adoption of cybersecurity [52]

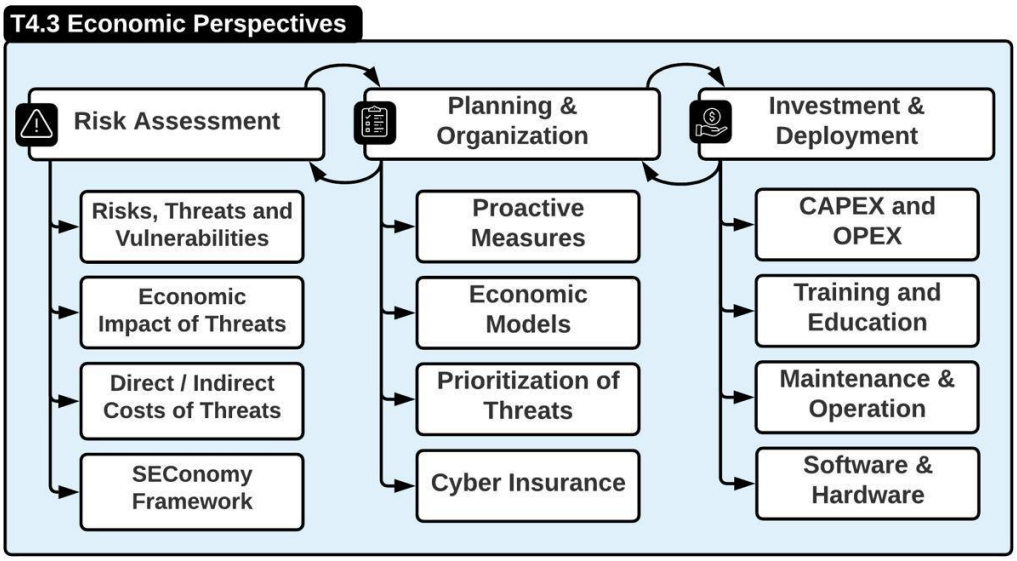


Figure 4: Overview of the T4.3 dimensions

Figure 4 highlights the different dimensions and activities being explored by T4.3. The risk assessment remains a key factor for the economic analysis since understanding a system's threats is critical for a precise diagnosis. Based on the full picture of the possible threats, economic analysis can estimate economic impacts on the system or the supply chain a system is a part of. Next, the Planning and Organization of cybersecurity involve deciding about different solutions that will compound the cybersecurity strategy to be adopted, including the decision regarding which threats to focus (e.g., invest to avoid Ransomware, assume the risks of a DDoS attack, and contract cyber insurance to reduce financial loss due to cyberattacks). Finally, the investments effectively should be made in order to deploy the cybersecurity strategy, which includes Capital Expenditure (CAPEX) and Operational Expenditure (OPEX) related costs to acquire, maintain and operate the protections (both software and hardware) and also the costs of training the personnel to adopt the defined cybersecurity strategy.

In the first year of the CONCORDIA, the work developed within the T4.3 focused on the risk assessment and planning of cybersecurity. For that, it was introduced the SEConomy framework [53] for applying economic models that take into account risks and threats attributed to each stakeholder's role within an ecosystem. SEConomy has guided the development of different approaches and tools for a structured risk assessment, planning, and cybersecurity investments with an economic bias. These approaches have been used as

a basis to implement new approaches in the context of T4.3, such as the SERViz, MENTOR, and SecBot, as described in detail in the next sections.

This chapter is divided as follows. SERViz, a visual tool for analyzing risks and planning investments in cybersecurity, is introduced in Section 5.1.1. Next, in Section 5.1.2, MENTOR is presented as a recommendation system to help decide which solution provides a proper protection level according to the specific business requirements (*e.g.*, budget and technical aspects). Then, a conversational agent named SecBot is introduced for the support of the adoption of cybersecurity by companies and also to guide non-technical users through cybersecurity issues. The SecBot takes into account the main challenges, limitations, and requirements of the Small and Medium
Enterprises (SME) sector. For each of the new approaches presented, different case studies have been conducted to show their feasibility. Finally, in Section 6.3, the conclusions and future steps of the T4.3 are discussed.

5.1 New Approaches

5.1.1. SERViz: A Visual Tool for Cybersecurity Investments

To invest in cybersecurity, it is critical to know which measures provide the greatest possible security in the future. So proactive measures are measures taken in the present to prevent greater damage in the future. SERViz, a visual tool, based on the SEConomy framework (as provided for CONCORDIA Y1 the context of T4.3), is introduced as an effort to address part of the identified challenges and help decision-makers during the cybersecurity investment planning. By using SERViz, decision-makers can set parameters, evaluate their current system, and make a risk assessment. It was proposed to be easily extended to support different information and scenarios according to the requirements of the sector or company being analysed.

The solution allows for calculating the overall level of business vulnerability and the most common risks for this sector. It also provides an estimation of the direct and indirect costs of this attack based on reports from sectors involved. After that, proactive measures are provided to help the decision-maker understand how to improve an IT system's security level. In detail, for each proactive measure selected, the Return on Security Investment (ROSI) for the business is calculated, considering the budget available and the cost of this measure. A case study considering a ransomware attack in the Healthcare sector was undertaken to exemplify an interaction with this tool. Further case studies are foreseen to address different sectors.

5.1.1.1. Approach and Prototype

The main goal of SERViz is to simplify the process of understanding the risks and possible investments in a business, taking into account general information available and the market trends. A web-based user interface is provided to users to interact and obtain insights for more accurate planning. It is also important to mention that SERViz implements a dynamically generated interface according to the information mapped according to the tool’s selected parameters as of those provided below. Thus, extending the supporting information and applying changes directly to how the different metrics and risks are used for the different calculations are possible. Therefore, although SERViz stands by now as a

Proof-of-Concept (PoC) tool [54] new scenarios and information can be covered to address more realistic scenarios. To design the tool, it was important first to define the requirements of the decision-makers. Based on a literature review and analysis of different stakeholders, the following parameters were selected:

- **Threat Type -** This parameter gives information on which type of threats the tool covers. The user can choose the type of threat from a drop-down list. Ideally, the user already knows the existing threats and which threats are most relevant for the organization. So that the user can choose the most important one. Examples of cyber threats are DDoS, Ransomware, and Phishing.
- **Business Sector** - The user has to choose which business sector his organization is. Possible business sectors are, for example, Healthcare, Finance, and Information technology. By choosing a business sector, the tool can provide more accurate information because the cost and risk of an attack are very different for each business sector.
- **Proactive Measures** - After choosing a threat type, the tool provides for the user a drop-down list of possible proactive cybersecurity measures against the selected cyber threat. The user can select one or several measures to get further information about them. Let us assume the user selected, as threat type, a ransomware attack. Some possible proactive measures would be Access Control, Disaster Recovery Plan, or Data Backup.
- **Budget** - As the name indicates, the budget parameter defines how much money the user is willing to invest in one or several cybersecurity measures. Once a user has chosen a proactive measure, he can define a budget for the measure, and the tool will provide the ROSI.
- **System Evaluation** - Dependent on the type of threat the user has selected, the tool will ask different questions about the users' systems to determine how vulnerable the system is to the chosen threat. For example, if the user has chosen, as threat type, a ransomware attack, one question from the system evaluation would be "Type of Operation System" or "Last time a backup was executed". It is assumed that the user knows the current status of his system in use.

These parameters are important in order to present information to the user as precisely as possible. They provide flexibility for decision-makers to compare outputs by setting different parameters. For example, the user can set the parameter *Budget* for various proactive measures to compare the calculated ROSI, thus helping the user during the investment decisions.

To make a risk assessment as accurate as possible, it is very important to evaluate the user's systems (*i.e.,* technology, operating system, and underlying infrastructure). To know if the user should invest in cybersecurity, it is important to check how vulnerable the system is to certain threats. If it turns out that the system is already very secure, because in the past the organizations already invested much money into cybersecurity, may no further investment is needed. On the other hand, if the evaluation shows that the system is very vulnerable, the user is informed and can invest in cybersecurity. For every cyber threat included in the tool are the corresponding cybersecurity measures saved in the database. As illustrated in
Figure 5: Example of a system evaluation mapping for backups, every measure has associated sub-measures, and the sub-measures have different options, which are also mapped in the database.

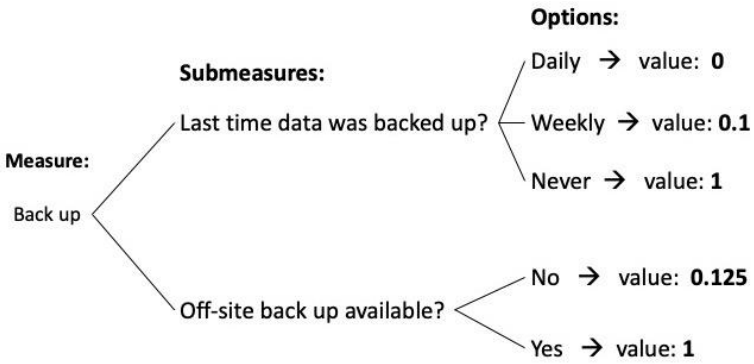


Figure 5: Example of a system evaluation mapping for backups

The sub-measures are shown as input parameters and the user can choose one of the associated options in the form of a drop-down selection. Every option has an associated weighted value between [0, 1] stored in the database. The weighted value represents how much of an impact the existence or non-existence of a cybersecurity measure has on the system's vulnerability where the number zero represents the highest level of security and one the lowest level. The weight values are based on research and estimates related to a specific cyber threat and are always open for improvement if the research data changes or more data is available.

To calculate the metric for the system vulnerability, every weight value (*W*) is added up and divided by the number of weight values, which results in the average weight value for the whole system. This metric, as introduced in Equation 1, is defined as *Alpha*.

$$Alpha = \frac{(W1 + W2 + W3 + ... + Wn)}{Number\ of\ weight\ values} \quad where\ Alpha \in [0, 1]$$

Equation 1: Calculation of Alpha for the risk assessment

Alpha is ranked into three different levels to give context to the calculated number. If it is between [0.15, 0.4], the system's vulnerability is low concerning a specific cyberattack. On the other hand, if *Alpha* is between [0.41, 0.7] or [0.71, 1], the system's vulnerability is medium or high, respectively. Another important part of the risk assessment is the possible impact of a cyberattack on the organization when a vulnerability gets exploited, and an attack would happen. The following metrics are mapped in the database for each cyber threat. The direct cost represents the estimated financial consequences of one associated cyberattack and is based on the statistical average cost. It can include, for example, downtime cost, recovery cost, and cost of data loss.

Besides that, indirect costs cannot be disregarded. In many cases, the indirect costs have an even more severe negative impact on the organization than the direct costs. As the quantification of indirect cost is not a challenging task, it was ranked in three stages to simplify the process. There are *Low*, *Medium*, and *High* estimated indirect costs. One of these three possibilities is mapped in the database for every cyber threat. In this solution, the direct costs are mainly dependent on the affected business sector and are based on statistics and research. The business sector is a key factor in how high the indirect costs for

an organization are. Examples of indirect costs are loss of reputation and confidence, which are worse for organizations in specific business sectors than others.

The metric used in the tool to support the decision making for cybersecurity investment is based on the ROSI model. It offers a benchmark to determine when a particular investment in a cybersecurity measure is recommended based on the potential financial loss, mitigation of the risk, and the solution's cost. As shown in Equation 2, instead of risk exposure, the formula uses the *Direct Cost* stored in the database. Of course, the *Indirect Cost* should also be a part of the risk exposure, but since it is impossible to quantify it, the solution considers only the *Direct Costs*.

The cost of the solution is replaced with *the Budget for the measure*. Thus, the user can enter how much he is willing to invest in a particular measure. The user himself has to clarify whether it is possible to carry out the measure with the budget set.
To determine the variable *Risk Mitigation Factor* is challenging because there is no data available on how much one measure mitigates an attack's risk. As a solution, we used the formula for the *Alpha*, which represents the system vulnerability. As Equation 3 shows, *Alpha* is calculated once with and once without the measure, and the weight values of all the other measures are kept constant. The difference provides the *Risk Mitigation Factor* (RMF) of one measure and is mapped in the database for every measure.

$$Risk\ Mitigation\ Factor = Alpha\ with\ Measure\ -\ Alpha\ without\ Measure$$

Equation 2: Risk Mitigation Factor calculation

The ROSI metric shows how much (in percentage) of the cost could be saved by implementing a security measure. If the ROSI is positive, it is recommended to invest and not if it is negative. The Equation 3 is used to calculate the ROSI for one measure, but the tool also provides a ROSI whether the user wants to invest in several measures, as is presented in Equation 4. Direct Costs stay the same, but it adds up all the RMF of all the measures the user wants to invest in.

$$ROSI = \frac{(Direct\ Cost * \ Risk\ Mitigation\ Factor) - Budget\ for\ the\ measure}{Budget\ for\ the\ measure}$$

Equation 3: ROSI calculation as being used to the SERViz

$$ROSI = \frac{(Direct\ Costs * (\ RMF1 + \ RMF2 + .. + \ RMFn) - Total\ Budget}{Total\ Budget}$$

Equation 4: ROSI calculation as being used to the SERViz for more than one measure

Thus, based on the defined use cases and the risk assessment described, the decision-makers can interact with the platform. First, the decision-maker configures the two inputs, threat type, and business sector. Dependent on these inputs, forms for the system evaluation will be shown to the user. After submitting the forms for the system evaluation, the alpha is calculated and shown along with the user's different costs. Next, the user can choose

between one or several proactive measures associated with the cyberattack, set a budget, and the tool calculates the ROSI. A pie chart that shows the distribution of the targeted business sectors by the chosen threat is also provided.

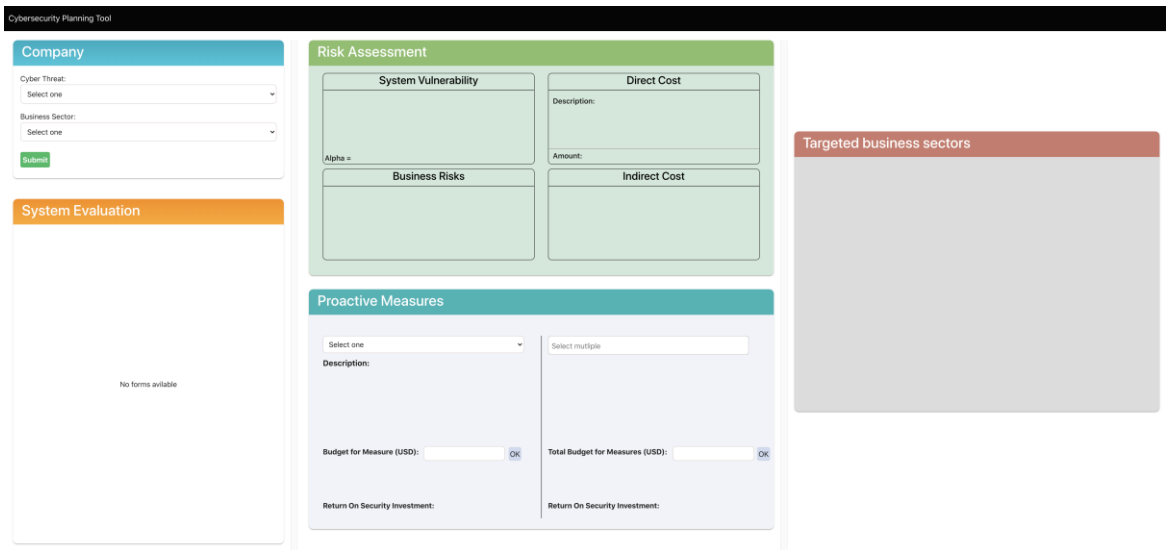


Figure 6: Overview of the SERViz without information and assessments

Figure 6 shows the dashboard of SERViz. First, the user defines the business sector and the type of attack to be analysed. After submitting such information, the System Evaluation tab is populated with the corresponding form for that sector and attack (*cf.* Figure 8). Next, the Risk Assessment is provided based on the information selected in the system evaluation form. Finally, the user can decide for different proactive measures and define the budget available to calculate the ROSI for that specific – or multiples – proactive measures. Further, a pie chart (*cf.* Figure 10) is provided on the "target business sectors" tab to show the average of the defined type of attack for each sector.

5.1.1.2. Case Study #1 – Risk Assessment

For this case study, let us consider the user of the tool is the IT project leader of a hospital. He/she has the responsibility and makes the decisions regarding all the IT. One day, the hospital management approaches the IT project leader and talks about concerns regarding the steady increase of cyberattacks lately, especially in the healthcare sector. The user read in the news that many hospitals have to deal with ransomware attacks and some of them suffered much damage from it. The management wants to know from the IT project leader how well prepared respectively how secure their system is concerning ransomware attacks or if the system has to be improved and the possible impact in case of an attack. Keeping that in mind, the IT project leader will use the proposed tool to support him with the given task.

First, the user will set the two parameters in the company tab (Figure 7). There he/she can choose a cyberattack and the relevant business sector from a drop-down menu. In this case, the user chooses healthcare as the business sector and ransomware as an attack type.

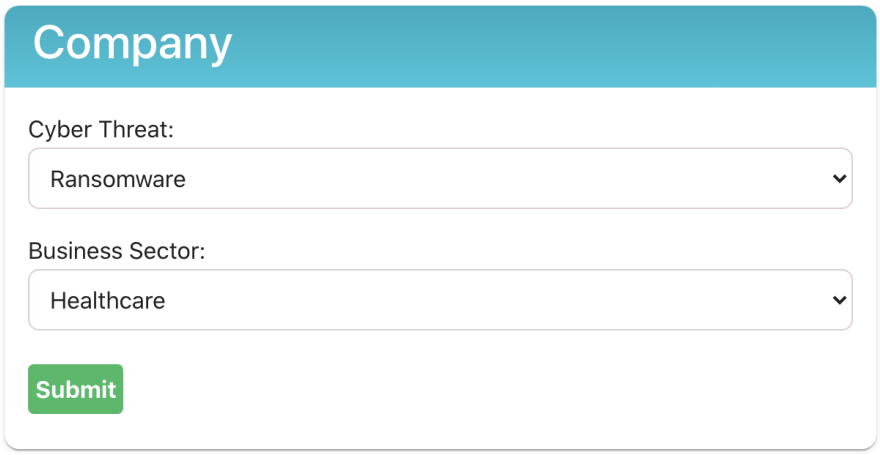


Figure 7: Company Tab

After submitting the company tab's parameters, the forms for evaluating the vulnerability of the system concerning a ransomware attack are shown. In Figure 8, the options are set to default values, representing the worst-case (i.e., highest vulnerability of the system). Let's assume the user keeps the options like that and this would be an accurate representation of the hospital's system. The *Alpha* calculation for this system is equal to 1 for this case. This would mean that the system of the hospital is highly vulnerable to ransomware attacks and, in the past, has never been made any investments in cybersecurity measures. Consequently, it is highly advised to inform the hospital's management about the lack of security, and a budget for cybersecurity investment should be provided.

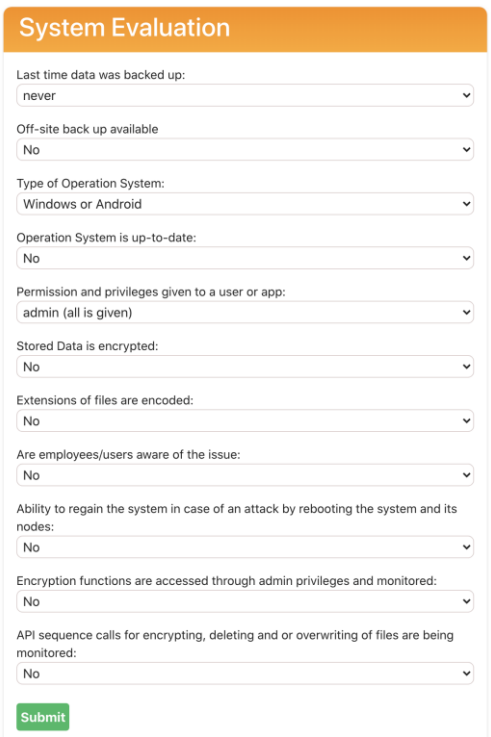


Figure 8: System Evaluation form for a Ransomware scenario

After submitting them, the data is shown in all the other tabs. The risk assessment tab with the data (Figure 9) is shown, which provides the *Alpha*, respectively, the system vulnerability, direct cost, indirect cost, and business risks. As shown in Figure 9, the *Alpha*, in this case, is 0.69, which represents, according to the alpha ranking,

a *Medium* vulnerability of the system. It means that the system is not highly vulnerable, but it can still be improved. On the upper right tab (Figure 9), the user can see the possible financial impact of a ransomware attack in healthcare, which is roughly €120,000. Besides, he/she can see that the indirect cost would be *High* because of the reputation damage and confidence loss of the hospital. The targeted business sectors tab (*Figure 10*) also provides useful information for the risk assessment. When the user hovers over the graph's healthcare sector, it shows the user that 13.6% of all the ransomware attacks are targeting the healthcare sector. Thus, the healthcare sector is the third biggest sector in the graphic.

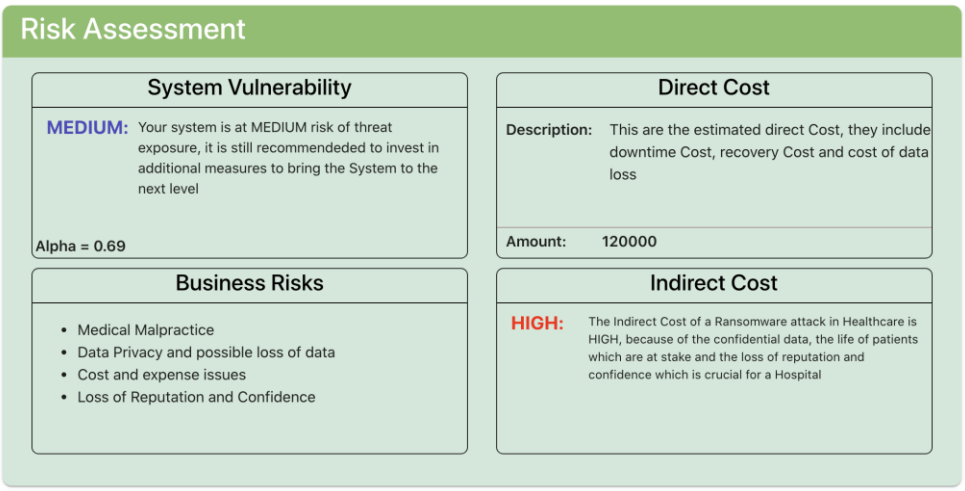


Figure 9: Risk Assessment for the Case Study #1

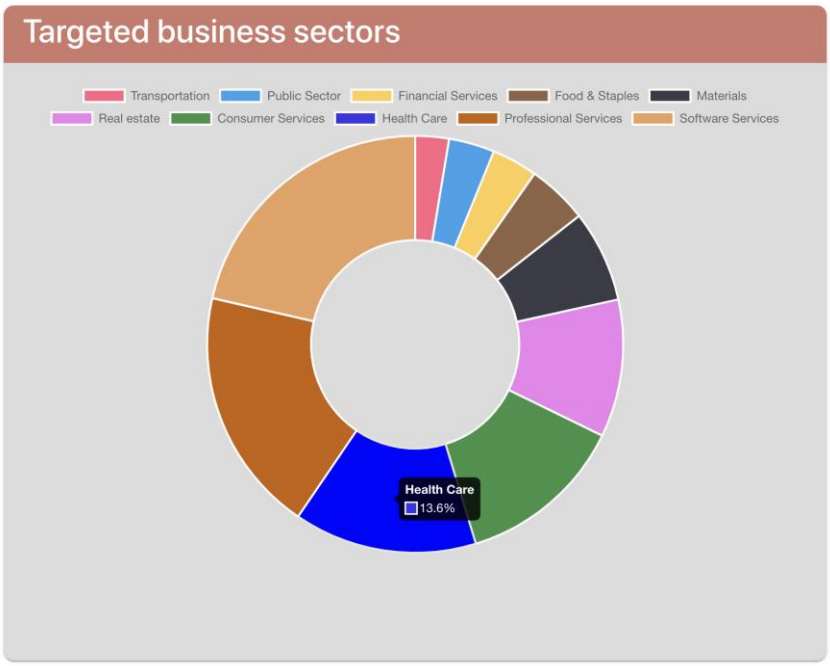


Figure 10: Overview of the most common targets for a Ransomware using arbitrary information

With all this information, the IT project leader can go to the management and provide useful information about the current system's security and the possible impact a ransomware attack could have. This information provides a good foundation for cybersecurity investment decisions and the management can decide whether they want to provide a budget to invest in additional measures.

5.1.1.3. Case Study #2 – Investments

For this case study, let us assume the hospital's management team decides, after seeing the data presented in Case Study No. 1, to improve the security of the system against ransomware attacks. The management provides a budget of €10,000 and advises the IT project manager that he should invest the budget in order to provide the highest ROSI. To help the user making cybersecurity investment decisions, the tool provides the proactive measure tab (Figure 11).

On the left side of the proactive measure tab, the user can choose one measure against ransomware, read the description of the measure, set the budget, and calculate the ROSI. In Figure 11, the user chose the measure Access Control, which is one of the measures not provided in the hospital system yet. If he/she sets the total budget of € 10,000 for only this measure, the tool calculates a ROSI of -16.00%. This means that if the implementation of the measure Access Control would cost € 10,000 and thus use up the whole budget, it is not advised to invest in the measure. Based on the second measure, as shown in Figure 11 on the left side of the tab, the user chooses Cyber Insurance as a measure with an assumed coverage rate of 90% and sets the budget again on € 10,000. The calculate Return on Security Investment is 980% and it would be advised to invest in Cyber Insurance.

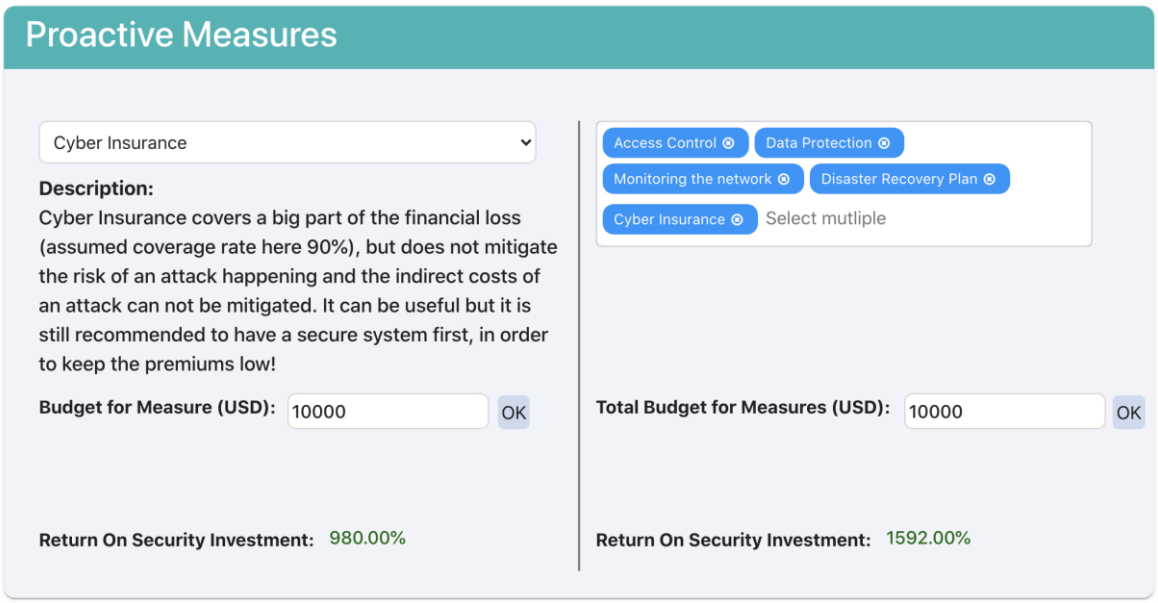


Figure 11: Proactive measures for the Case Study #2

On the right side of the proactive measures tab the user can choose several measures and set a budget and calculate the ROSI. The user selects as shown in Figure 11 all the additional proactive measure that the hospital does not have and sets the total budget of € 10,000 and the tool provides the ROSI of 1592%. This means that if it is possible to implement all these measures with the budget of € 10,000 it would be highly advised to invest in all the missing measures.

The IT project manager can inform the management that investing in all these measures would provide the highest ROSI but first, they have to clarify how much it would cost to implement these solutions for the hospital in order to verify if it is possible with the set budget. If it is not possible, they either have to increase the budget or implement fewer measures.

5.1.1.4. Current State and Limitations

The two case studies deal with the two different main concepts provided by the tool. Both the risk assessment and the investment in cybersecurity aim to be simplified in the proposed solution. The critical information is provided to the user with a graphical and interactive user interface for the cybersecurity risk assessment and investment. The user gets an idea of the risk his organization is exposed to and possible investment strategies he/she could implement. One of the tool's limitations is that the user can only choose one cyber threat and has to do the cybersecurity risk assessment and investment separately for every threat. If the user could choose several threats at once, it would make the tool a lot more complicated because the system evaluation would be very long. The user had to select forms for every threat and a dependency between the different cyberattacks. The risk of one cyber threat impacts the risk of another one, and there is a possible cascade failing, which is not considered in the tool.

Another limitation of the tool is the accuracy. The mapping of the different weight values for the risk assessment calculation (*i.e.*, Equation 1) depends on research. It is challenging to define them so that they represent reality because the research data is limited. The tool depends on the weight values because they are used to calculate the *Alpha* and the *Risk Mitigation Factor*, which significantly impacts the accuracy of the ROSI metric. Also, the accuracy of the direct cost and indirect cost is dependent on the research data. If the data is not available, it is not possible to make an accurate risk assessment. As shown in Case Study #2, the user has to find out how much the implementation of specific security measures would cost. If there would be accurate data available on how much it costs to implement specific measures, they could be mapped to the database and the user has only to set the budget without doing any research about the cost of the measures. Currently, the user's set budget represents the cost of the associated measure because of the lack of available data.

5.1.2. MENTOR: On the Recommendation of Protections

Currently, companies invest in protection services (*e.g.*, firewalls and anti-malware tools) and response teams to ensure availability and protect critical services and infrastructures. The cybersecurity market is worth billions of euros and investments are steadily rising. Thus, there are financial incentives for Protection Service Providers (PSP) to enter the market by offering protection services while end-users can reduce protection costs (*e.g.*, related to the deployment, configuration, and operation of services) by leveraging a competitive market for cybersecurity to meet their specific demands. These protections may include the acquisition of physical appliances, software licenses, virtual network functions, and cloud-based protection. Thus, although traditional models will still meet specific demands, a notable amount of next-generation protection services -- as an instance of cybersecurity management -- can adapt to flexible business models and provide a different level of protection on-demand.

Thus, there are a number of on-demand protection services and marketplaces available, which are not only offering protection services, but also offer alternatives regarding the deployment and management aspects of such services. However, it is not a trivial task for end-users to select one of them. Decision-making is even more critical when infrastructure is under attack and the decision to mitigate the attack should be provided on the basis of information about the infrastructure, such as its economic aspects, demands, and the characteristics of the attack. In this scenario, it is essential to observe not only how often

attacks surpass the on-site infrastructure capacity, but also which off-site services can provide the necessary protection, considering their different service flavours, such as the amount of traffic supported, the capacity to address particularities of a determined attack, and price conditions. In this sense, recommendation systems provide a valuable security management tool to support decision during the detection and mitigation process.

Therefore, MENTOR [55] a protection service recommendation system, is proposed as a support tool for cybersecurity management, being able to recommend services for the prevention and mitigation of cyberattacks. This work investigates similarity measure techniques to correlate information, such as budget constraints and the type of service required, from customers with different services available. Based on this, MENTOR is able to indicate an adequate service to protect infrastructures according to different demands, such as region, deployment time, and price conditions. Such services are based on state-of-the-art technologies, providing features to deliver, according to previous configurations, different levels of performance, security, and availability. In addition, an evaluation and discussion determine the performance and accuracy of each similarity measure technique implemented within MENTOR.

5.1.2.1. MENTOR's Approach

The MENTOR system assists network operators during the decision process on measures to protect critical infrastructure, thus performing an important security management task. For this, the recommendation engine indicates protection services available from different PSPs to prevent and mitigate threats. Different properties from available protection services, the customer profile, and characteristics of the cyber attack are used to establish a fair recommendation system. Thus, one or more services from different PSPs (*e.g.*, both small companies and global players) can be proposed to neutralize a threat efficiently, while minimizing cost and reducing damage.

The process overview of MENTOR is depicted in Figure 12. One customer can describe his/her requirements (*e.g.*, budget, threat, and type of protection service) that can be used by the system to filter the content of available services from different PSPs in order to determine which one is most suitable to support all requirements and demands described. Different similarity algorithms are applied by the recommendation engine to determine the most appropriate service for the customer.

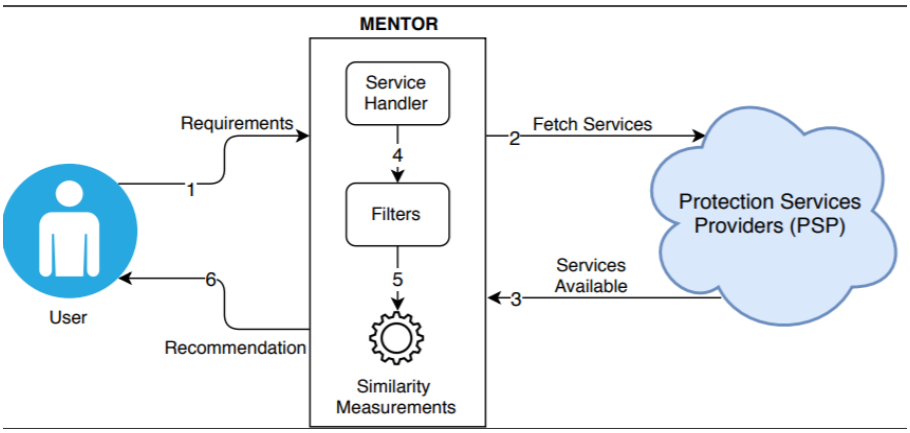


Figure 12: Recommendation process overview

Figure 13 overviews the architecture of MENTOR. The recommendation flow is described as follows. First, in step 1, the *Service Requestor* receives information related to the infrastructure under attack and characteristics of the attack (*e.g.,* logs from monitors). Such information is transformed into an appropriate data structure and delivered to the *Extractor*, which initializes the recommendation process. Next, in the Extraction and Classification phases (steps 2 and 3), the information is analysed and correlated with the type of attack in order to identify those requirements, which fend off the attack. In turn, a list of potential protection services is generated (step 4) and forwarded (step 5) to the recommendation engine. Finally, in step 6, the recommendation engine uses the customer profile input to define, which service from the list, is the optimal recommendation. Details about components that execute such actions in each step of the system are as follows.

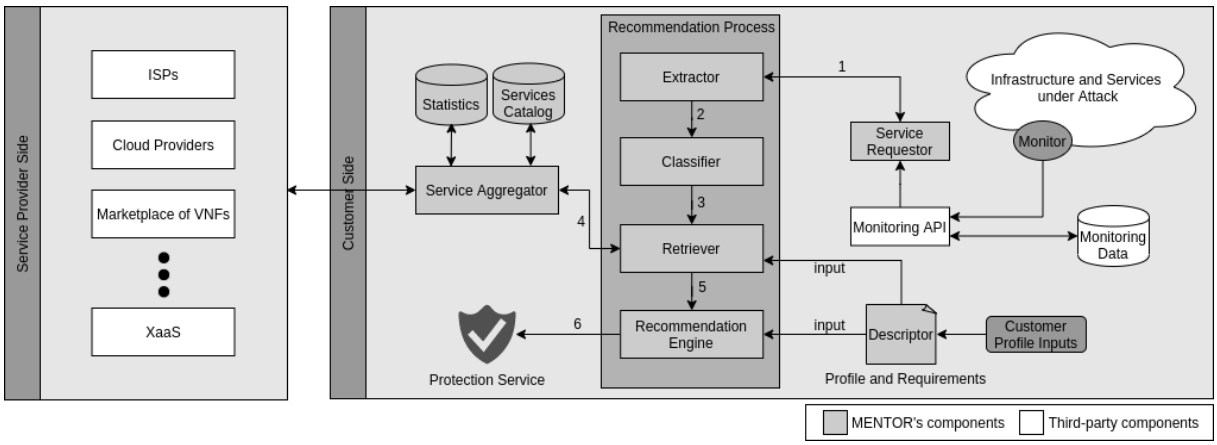


Figure 13: MENTOR's conceptual architecture

In the first step, the *Service Requestor* receives data from monitors, stores relevant data in a database for future analysis, and, when a threat or imminent attack is identified, the component sends the significant information and meta-data to the *Extractor* component to start the recommendation process. Next, the *Extractor*, which is the first step of the recommendation process, is in charge of extracting relevant insights (*e.g.*, attackers, attack characteristics, and infrastructure impacts) from the data monitored. After the extraction, the information is forwarded to the data categorized into different kind of attacks.

During the next phase, the *Classifier* is responsible for classifying the extracted data according to the previously reported and identified attacks (*e.g.*, DDoS variations). To achieve this classification, techniques to identify attacks patterns and also a database providing attacks fingerprints are applied. After the classification, the *Solutions Aggregator* communicates with different PSPs to obtain a list of available services available and relevant properties of each service (*e.g.*, price, type of service, and coverage area). Next, the database containing the services catalog is populated to supply customers. The list of PSPs can be modified according to customer preferences. Then, the *Retriever* is in charge of querying the *Solutions Aggregator*, who can fully or partially address the demands of the end-user. Such services selected and returned can yield different solutions targeting the same problem, but can vary in terms of performance, price, and the technology being used.

The final step of the recommendation process is composed by the *Recommendation Engine*, which supports different algorithms to select the optimal service, based on the list provided by the *Retriever*. Besides the input provided by the *Retriever*, a set of details is described

by the customer to map the end-user profile and requirements. Therefore, to support such a decision, different aspects have to be considered, such as budget constraints, service coverage, and the capacity to address the particularities of an attack.

5.1.2.1.1. Recommendation Engine

The input data for the recommendation engine depicts a list of available protection services from PSPs. This list contains general information about the service (*e.g.*, price and type of service) as well as technical details regarding threats and attacks supported by each service. The data returned by each PSPs should optimally be provided through an interface (*e.g.*, RESTful API) to communicate with MENTOR's *Solutions Aggregator* in order to be incorporated into the recommendation process. Thus, providing such an interface is in the interest of every PSP.

Table 20 presents those parameters that define the requirements of the end-user running the recommendation system. These parameters are to be defined inside a profile and requirements descriptor (*e.g.*, a JSON file), containing useful information used during the filtering and recommendation steps conducted by the *Retriever* and the *Recommendation Engine*. One end-user, for instance, can use such descriptor to configure the recommendation system to temporarily contract a reactive virtual protection service being remotely hosted in South America, with a deployment time of just a few seconds. The amount available to spend on such service will be defined as 500 *EUR*. Also, if available, information about an imminent attack or threats possible to be exploited can be described. Thus, based on this information, protection services that do not support all requirements will not be considered as a viable option. As the recommendation system is able to adapt to different input scenarios, the descriptor can also be extended to support new parameters and relevant information provided by the protection services available, such as attack's behaviours or vulnerable applications.

Table 20: Customer profile and Requirements

Parameter	Description	Value
Type of Service	Describes if there is a demand to protect the network from further threats (*i.e.*, proactive) or react in order to mitigate imminent attacks (*i.e.*, reactive)	reactive or proactive
Type of Attack	Provides details of the attack which a protection is being required	*e.g.*, SYN Flood or a specific malware
Attack Details	Uploads log files or details about the attack	*e.g.*, DDoS fingerprints or behavior data of any attack
Region	Defines specific geolocalization that one protection service should be deployed or able to act	continent, country, city, or any
Deployment Time	Describes the maximum time between the service being contracted until it be able to protect the customer	seconds, minutes, hours, days, or any
Leasing Period	Defines the period for which the customer want to contract a protection service	minutes, hours, days, weeks, months, or any
Budget	The amount (*e.g.*, in Euro or USD) available to spend with protection	any

In order to evaluate the feasibility of the recommendation process, the MENTOR was assessed using four widely used similarity measures: *(i)* Euclidean distance, *(ii)* Manhattan distance, *(iii)* Cosine similarity, and *(iv)* Pearson correlation. These measures were selected because of their potential to quantify the similarity of two objects. Thus, end-users demand can be compared with protections available in order to decide which fits better for each

specific case. MENTOR was designed to be generic and extensible to support further algorithms to recommend protection services. In this regard, service requirements from customers and offered protection services are mapped as vectors in space as depicted in Figure 14, *i.e.*, their set of attributes as well as magnitudes represents a direction in space, allowing a geometric evaluation of similarity.

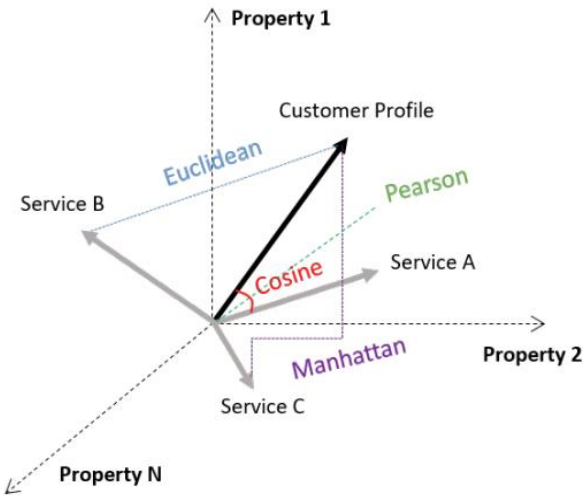


Figure 14: Protection services mapped into vectors and compared to customer profiles using different similarity measures

Equation 5(1) presents the Euclidean distance. The Euclidean distance is calculated by taking the square root of the sum of the squared pair-wise distances of every dimension. In terms of the recommendation process, a vector containing the parameters defined by the end-user (*cf.* Table 20) are described as a vector x_i and each service available is transformed to a vector y_i in the same way. Then, the sum of differences of all individual squared pair-wise distances is square rooted. Thus, the Euclidean distance determines, if a service is adequate for the request: *i.e.*, the optimal recommendation is the service with the lowest possible Euclidean distance. In a similar approach, the Manhattan distance, introduced in Equation 5(2), calculates the distance (*beta*) between two vectors by considering the difference of the absolute values of each vector. The vector *X* represents the protection service and *Y* the end-user profile. The best service is the one with the shortest diagonal path between the two vectors. Similar to the Euclidean distance, the protection service with the lowest possible value is optimal.

Equation 5 (3) shows the Cosine similarity calculation, which finds the normalized dot product of two attributes *X* and *Y*. *Cos(x ,y)*, where *X* is any dimension of the end-user request and *Y* is a dimension of a protection service), is calculated between the two vectors to decide, if one service fits the end-user request. If the angle is equal to 0 degree, the value for the cosine will be 1 (best recommendation) and it is less than 1 (*i.e.*, it ranges from 0.99 to -1) for any other angle. The fourth measure under investigation is the Pearson correlation (*cf.* Equation 5(4). The Pearson correlation determines linear relationships between two normalized distributed variables. This correlation provides a value ranging from -1 to 1, representing the correlation between two vectors. Thus, the lower the value, the worse is a protection service *X* recommended for a demand *Y*.

$$euclidean(x,y) = \sqrt{\sum_{i=1}^{n}(x_i - y_i)^2} \quad (1)$$

$$manhattan(x,y) = \sum_{i=1}^{n}|x_i - y_i| \quad (2)$$

$$\cos(x,y) = \frac{\sum_{i=1}^{n}(X_i \cdot Y_i)}{\sqrt{\sum_{i=1}^{n} X_i} \cdot \sqrt{\sum_{i=1}^{n} Y_i}} \quad (3)$$

$$pearson(x,y) = \frac{\sum_{i=1}^{n}(x_i - \overline{x})(y_i - \overline{y})}{\sqrt{\sum_{i=1}^{n}(x_i - \overline{x})^2 (y_i - \overline{y})^2}} \quad (4)$$

Equation 5: Correlation Similarities

The recommendation process works as depicted in Algorithm 1. Initial preparation steps involve *(a)* receiving/preparing input data and *(b)* filtering unrelated services. The input *(a)* requires receiving protection services from the *Solutions Aggregator*, which for the purpose of evaluation were created randomly. Next, the customer profile is determined (*i.e.*, received from the front-end or to establish the basis of comparison those services offered for protection. Before calculating similarities, unrelated services are discarded in the filtering process. This involves eliminating services, whose binary properties do not match the ones required by the customer, *e.g.*, type of service (reactive or proactive) or service region (Europe).

```
1  begin
       /* Receive services from Aggregator        */
2      services ← get_services()
       /* Receive customer requirements           */
3      profile ← get_customerProfile()
       /* Get customer index                      */
4      profile.index ← index(profile)
       /* Step 1 - Filter Unrelated Services      */
5      services ← filter(services)
       /* Step 2 - Recommend Remaining Services   */
6      for each s ∈ services:
           /* Get index of each service           */
7          x ← index(services)
8          y ← profile.index
           /* Step 3,4 - Calculate and store
              similarities                         */
9          cosine[] ← s.cos ← cosine(x, y)
10         euclidean[] ← s.euc ← euclidean(x, y)
11         manhattan[] ← s.man ← manhattan(x, y)
12         pearson[] ← s.pea ← pearson(x, y)
13 end
```

Algorithm 1: MENTOR's Recommendation

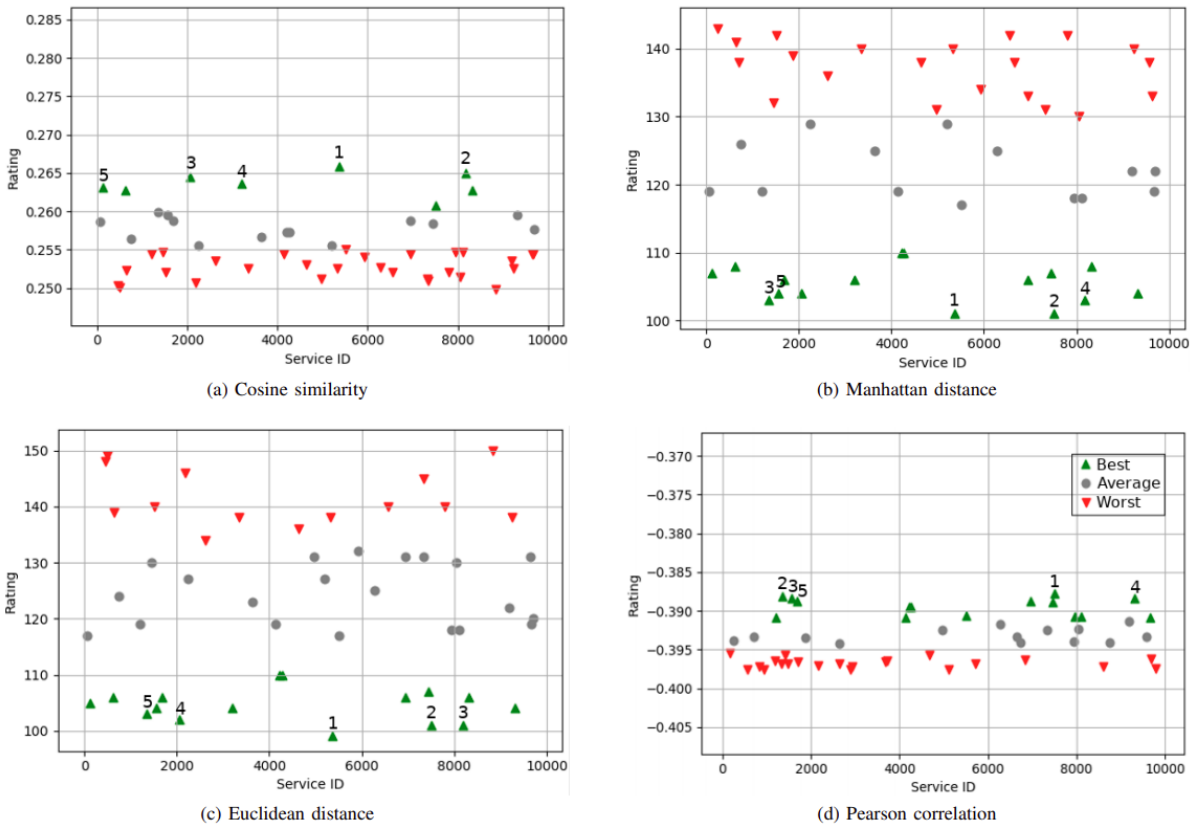
Step 1 involves the indexing of *(a)* service parameters required by the customer and *(b)* each service in order to build an integer array representing the service. These steps are necessary to map services and enable the application of similarity measures geometrically. Similarly, Step 2 is applied to each service to index its properties. Steps 3 and 4 involve the actual recommendation of services and storing of the rating. In Step 3, the customer profile is mapped as a vector *Y* and each protection services as a vector *X*, which are provided as input to similarity algorithms. In Step 4, ratings are stored as a similarity dictionary with the service ID as a key, especially to enable the export or plot similarity data later.

5.1.2.2. Evaluation

The dataset generated for the evaluation contains 10,000 randomly generated protection services, such as each service was described based on parameters available for the customer profile (*cf.* Table 20) and with a price range between 100 *EUR* and 1,000 *EUR*. Thus, by using such data as an input to the MENTOR, the performance and accuracy of the measurement algorithms to recommend protection services were analysed.

The four similarity measurements described beforehand were used to conduct this experiment. These requirements are indexed and translated into the vector composed by region, service type, deployment time, leasing period, and price, which is given as input to the recommendation engine. The customer profile (*i.e.,* input) was defined to represent a request for a reactive service against a DDoS attack, running in Europe with a deployment time in minutes, a leasing period in days, and the maximum budget to be up at 200 *EUR*. After the dataset's creation and the customer profile input, the recommendation engine applies a filter to discard unrelated services (*e.g.,* outside the price range, region, or deployment time). The similarity is calculated based on the given vector (*i.e.,* customer profile) by using each algorithm available on the current version of the MENTOR.

Figure 15 depicts the top fifty ranked services for each similarity algorithm, in which the best five are highlighted in Table 21. Although these recommended services were similar concerning the properties being compared, there are major differences in how these algorithms work depending on how the input vector is mapped. For example, all features of a protection service are described as a vector in space, in which certain properties can significantly change their direction, and consequently their rating. Therefore, high-magnitude variables (*e.g.,* price, deployment time, and leasing period) cause a major influence in the vector's direction in space, and thus, change the rating of its recommendation. For instance, a "worse" rating can be given to services that, in practice, may be better than those specified in the customer profile. That is, a service with a slightly higher price and a significantly lower deployment period may have a worse ranking due to the disparity, in absolute terms, between the properties of the protection service.



(a) Cosine similarity (b) Manhattan distance

(c) Euclidean distance (d) Pearson correlation

Figure 15: Ratings of the fifty best-ranked protection services according to each algorithm

Table 21: Summary of the five best-ranked protection services according to ratings calculated as of the figure above.

(a) Cosine similarity

Rank	ID	Rating	Price	Deployment	Leasing
1	5362	0.26585	100	Hours	Days
2	8182	0.26493	102	Seconds	Days
3	2062	0.26448	103	Seconds	Days
4	3202	0.26361	105	Hours	Days
5	122	0.26318	106	Seconds	Days

(b) Manhattan distance

Rank	ID	Rating	Price	Deployment	Leasing
1	5362	101	100	Hours	Days
2	7512	101	102	Seconds	Days
3	1352	103	104	Seconds	Days
4	8182	103	102	Hours	Days
5	1552	104	105	Seconds	Days

(c) Euclidean distance

Rank	ID	Rating	Price	Deployment	Leasing
1	5362	99.0202	100	Hours	Days
2	7512	101	102	Seconds	Days
3	8182	101.02	102	Hours	Days
4	2062	102.02	103	Hours	Days
5	1352	103	104	Seconds	Days

(d) Pearson correlation

Rank	ID	Rating	Price	Deployment	Leasing
1	7512	-0.38774	102	Seconds	Days
2	1352	-0.38814	104	Seconds	Days
3	1552	-0.38834	105	Seconds	Days
4	9312	-0.38834	105	Seconds	Days
5	1692	-0.38872	107	Seconds	Days

This is observed in the distance-based algorithms (*e.g.*, Cosine, Euclidean, and Manhattan in Table 21, in which the price was the most significant factor for the ranking of a service. For example, as observed in Figure 16, the service with ID 5362 was the service most similar to the vector specified by the customer profile (according to the distance-based algorithms), but it was not necessarily the best service. In this sense, services with a shorter deployment time (in the order of seconds) and without a significant price difference obtained a worse ranking due to the price difference. This happened for services ID 8182 and 7512 in the Tables of the Cosine, Manhattan, and Euclidean algorithms.

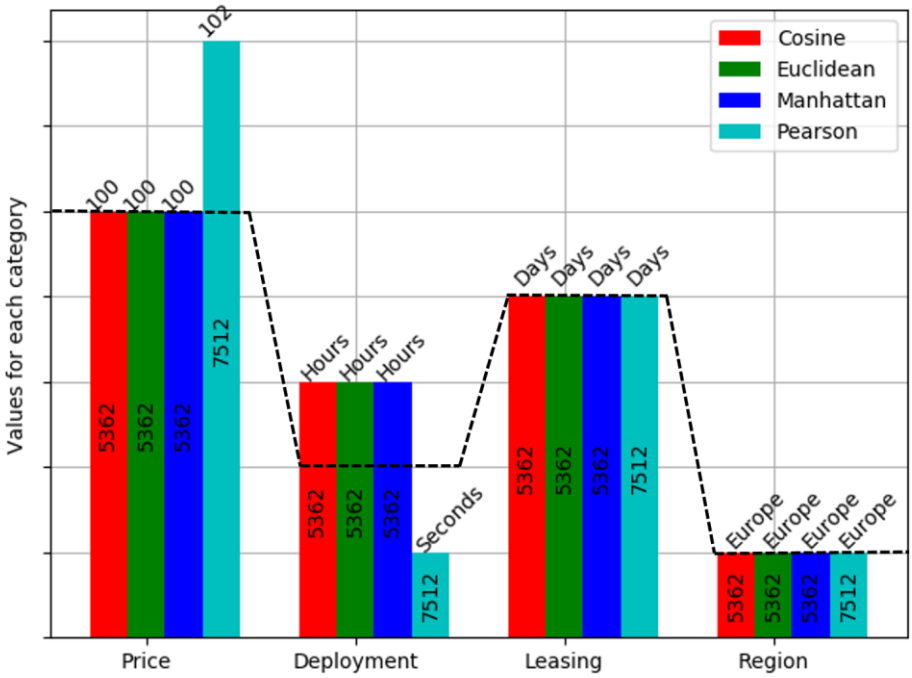


Figure 16: Best ranked solutions per algorithm in contrast to the customer profile represented by the dotted line

However, the major difference between the Pearson correlation and the distance-based algorithms is that it is invariant to the magnitude of elements. Hence, differences in service prices do not cause a major impact on their ratings because it mainly observes whether properties of protection services and the customer profile vary in a similar way. Thus, the service ID 7512 is recommended as the best service because they consider an insignificant increase in the price in contrast to a significant smaller deployment time. Therefore, considering the mapping of these characteristics of a protection service as a vector in space, the Pearson Correlation algorithm is presented as a generally better alternative in contrast to other distance-based similarity algorithms.

A possible alternative to circumvent these differences is given by grouping the vector of protection services for each attribute. Thus, it is possible to compare these service attributes with customer profile attributes in a 1-to-1 manner. Therefore, the final rating of a service is achieved by an average of the rating of its attributes. It should be noted, however, that attributes of protection services offering better conditions than those specified in the customer profile would receive worse ratings. Thus, an alternative can be a rearrangement of input attributes to the best possible conditions, making the recommendation algorithms offer the best alternative possible instead of the closer to the end-user request. For example, if one wants a protection service with deployment time in minutes, protection services a bit more expensive but with deployment time in seconds can be a most suitable recommendation since this still fits the budget and other requirements.

Lastly, such an evaluation indicates that MENTOR can recommend adequate protection services considering the price, geolocalisation, and other requirements defined by end-users. The distance-based algorithms recommended the cheapest service that is adequate for the end-user according to their demands. However, this service recommended is not necessarily the best one in terms of performance. The Pearson correlation decided toward a bit more

expensive service fitting the end-user's budget, while delivering the best performance possible.

5.1.2.3. Discussion and Limitations

Beyond the evaluation concerning the recommendation process provided above, others technical aspects and open challenges are important to be discussed in direction to improve MENTOR and also to shed light on further directions for cybersecurity research on the recommendation of protection services.

Although a large number of protection services are available in the market, this number will arise together with a global deployment of novel paradigms, such as NFV and SDN. Also, novel business models can be used as an incentive for the development of innovative cybersecurity solutions. Based on that, a recommendation system should be able to understand the nuances of services running on different technologies in order to recommend a service efficiently. Besides, mechanisms to deploy the service directly on the customer's infrastructure or in a third-party host should be available, thus simplifying the process of acquisition of such protection services by non-expert end-users.

For the MENTOR's evaluation, 10.000 possible protection services were randomly generated. Such services containing general information (*e.g.*, price, deployment time, and leasing period) helps to demonstrate the feasibility of the solution. However, those services do not represent the real amount of protection services available neither contains exhaustive information of protection services. Most studies should be conducted in order to create a data model (*e.g.*, descriptor) able to define different services and demands, which may include the categorization by technology supported, features provided, and performance aspects.

Also, the reputation of the PSP and protections services itself should be considered during the recommendation process. One should be able to verify the feedback provided by other customers as well as verify performance logs and issues related to past experiences. Besides that, mechanisms to apply penalties to PSP that does not meet the agreement demands should be considered. In such a direction, decentralized reputation mechanisms (*e.g.*, blockchain-based) can be developed to provide a trustworthy and immutable record of reputation regarding the protection services and its different vendors.

Another critical aspect of the recommendation system is related to the trust of customers to share data. This discussion is critical, and it is still an open challenge, not only for the MENTOR but for other work related to cybersecurity that demands real data to achieve an accurate output. Currently, as a proof-of-concept, it is assumed a consortium of companies and institutions that trust in each one. Thus, one trusted node receives data from customers and offers the MENTOR recommendation. Besides, the MENTOR is designed to run locally as well, which means that a customer can run his/her own instance of MENTOR in a private infrastructure, thus ensuring that the data will not be shared with third-parties.

Lastly, the process of recommending protection services assumes that end-users are able to provide data and the correct parameters to find adequate protection. However, in some cases, users may not know the kind of attack they are under so reactive service matching based on user input would be impractical. In addition, it is a challenge to integrate a recommendation system with a variety of logs, because, for example, there is no a single

standard of logs when concerning the different type of services and technologies. There is still a lack of mechanisms to deal with the deployment and management of different technologies in an integrated solution, such as APIs and wrappers that help to automate the deployment of recommended services without additional user' s interactions.

5.1.2.4. Summary, Conclusions and Next Steps

The MENTOR recommendation system maps different customers' requirements to recommend off-site protection services concerning not only price conditions, but also the capacity of services to address specific attacks. In addition, MENTOR leverages a competitive market, allowing end-users to acquire services from companies that openly announce their protection services. Also, a modular recommendation engine is provided to support further recommendations algorithms (as openly accessible code). The offering of a dashboard for human interactions in cybersecurity management tasks enables a practical and deployable solution. Since MENTOR does additionally offer an open API, the use of such a recommendation system within an existing Operation Support System (OSS) can automate decisions to be taken, too.

The mapping of the protection services as well as their attributes enables an accurate evaluation of the similarity between customer requirements and offered security services. MENTOR, in this sense, offers a viable approach for the recommendation of services (*e.g.*, possibly offered in open marketplaces based on blockchain).
Specifically, the Pearson correlation presented the best balance between cost/benefit considering the mapping of services as a vector. Therefore, in the defined implementation, non-binary characteristics have a significant impact on the evaluation of similarity in contrast to binary ones due to the order of their magnitude, which affects the direction of the vector in space, and as a consequence, its similarity rating.

5.1.3. SecBot: Cybersecurity Support for SMEs

Businesses becomes proportionally more exposed to cyberattacks as their reliance on Information and Communications Technologies (ICT) increases. As result, companies' investments in cybersecurity naturally increase. While large companies such as banks and governmental entities spend significant funds on adopting cybersecurity best practices and training dedicated technical personnel, Small and Medium-sized Enterprises (SMEs) often underinvest and lack efficient strategies to protect their Information Technology (IT) services and value chains they are part of [50] In addition, SMEs tend to show a misperception of their cybersecurity conditions, as a recent survey reveals. While 60% of US and UK SMEs believe their businesses are unlikely to be targeted by cyberattacks, the reality is the opposite, with a significant amount of breaches and cyberattacks targeting SMEs.

The adoption of efficient cybersecurity strategies in SMEs is challenging because of constraints mainly associated with the lack of a cybersecurity budget, unskilled human resources, and limited time allocated to cybersecurity planning. This can lead to disastrous impacts on business, including financial losses due to cyberattacks, mitigation of costs, and inefficient management of protections. From a human-centric perspective, simplifying the cybersecurity decision-making process requires clear and straightforward approaches for SMEs. It is essential to promote novel approaches that present cybersecurity technical information in an intuitive, user-friendly way, allowing less-skilled personnel to make

informed decisions while maintaining a proper level of protection of their businesses. SMEs can benefit from adopting faster and cheaper cybersecurity strategies, *e.g.,* by minimizing human experts' need while reducing costs by efficiently investing in defence mechanisms.

Conversational agents (*i.e.,* chatbots) have been recently highlighted as an ally to enhance business' cybersecurity adoption by sharing network and security information with non-technical staff. Advances in Natural Language Processing (NLP) --- driven by novel Machine Learning (ML) techniques --- led to conversational interfaces capable of extracting meaningful information and simplifying interactions between humans and machines. Compared to, *e.g.,* command-lines and technical dashboards, chatbots *(a)* provide a straightforward interaction using natural language, *(b)* enable faster decision-making, and *(c)* speed-up complex processes. The Cyber Helpline chatbot in the UK was proposed to provide immediate advice to citizens on how to deal with cybersecurity issues. However, even with those benefits, the employment of chatbots in the context of the SME cybersecurity is still scarce and limited to very specific scenarios. Hence, the current state-of-the-art neither fully covers the demands of SMEs nor considers barriers for cybersecurity adoption in SMEs (*e.g.,* awareness of standards, limited internal knowledge, and lack of clear implementation guidelines) [56].

In this context, SecBot [57] a cybersecurity-driven conversational agent, is introduced here to help non-expert users take informed and efficient cybersecurity decisions, reducing the risk of economic impacts due to business disruptions. For that, SecBot is designed to interact with non-experts to extract information on cybersecurity demands and business requirements. SecBot is able to *(a)* understand symptoms and business risks to correlate with potential cyberattacks, helping users comprehend incidents and their impacts, *(b)* provide recommendations for actions in different levels of abstraction, such as which efforts are required to avoid or to mitigate problems, and *(c)* support the configuration (*e.g.,* in-house firewall) or acquisition of protections, preparing actions (*e.g.,* command-lines or configuration files) required to configure or deploy a solution. The feasibility of SecBot is evaluated by conducting a case study and by analyzing its performance.

5.1.3.1. SecBot’s Solution

Two fundamental concepts are required for conversational agents: *Intents* and *Entities*. These concepts determine the basis to describe information and flows supported by SecBot. *Intents* refer to user's intentions when interacting with the chatbot, and *Entities* are defined to extract specific terms or values. Extracting entities and intent classification typically involves an ML architecture. While non-ML approaches do exist, they are normally outperformed by supervised learning algorithms, which can generalize the information extraction process by understanding the context of input phrases. In the case of SecBot, a Dual Intent and Entity Transformer (DIET) architecture [58] is used for intent classification and entity extraction, implemented by the Rasa framework [59]. The DIET classifier relies on a transformer neural network to encode input text with context, Conditional Random Fields (CRFs) to identify and extract entities from text encoded, and dot-product similarity to classify the input intent.

While *Intents* (*cf.* Table 23) identify users that want to find protection according to the budget available or want to ask for help to configure efficient protection, *Entities* are used to extract specific terms or values (*cf.* Table 22) from the user intent to provide a correct

response. To reach accurate responses, all entities are connected to knowledge databases, which describe values accepted for each of the specific entities. About 150 entries are defined for *Entities* (*cf.* Table 22) of SecBot. New entries for these *Entities* as well as new *Intents* can be added, such that the SecBot can cover different scenarios and demands.

After identifying the user's intent and extracting input entities from the input text, the SecBot needs to decide upon which action to take to best help the user. To that end, another important concept for conversational agents needs to be defined: *Stories*. A single *Story* defines those steps SecBot can take in response to a user's input, resulting in multiple possible conversation flows. For example, after recognizing the intent *attack_notification* and if the next one is the Intent *attack_details*, a message is sent asking for the budget available to invest in protection, before issuing a recommendation. However, if the next intent recognized is *problem_desc*, a different action will be executed to identify the type of attack. Thus, the definition of *Stories* is critical, given that it is used to train the solution to recognize the context of a conversation and to select the next actions or flows.

Table 22: Examples of Entities supported by the SecBot

Entity	Description	Input's Example
@attack_name	Name of the attack	I am being target of a @DDoS Attack.
@attack_type	Type of attack	It looks like a @SYN flood.
@target	Target of the attack or the component with symptoms	The target is my @Windows systems. It is my @database server.
@symptom	Describe specific problems or symptoms	My server is receiving @a lot of requests.
@budget	Amount and currency available to invest	My budget is @5000 EUR.
@solution, @technology	Describe in-house solutions	I have an @IPtables running on @Linux.
@operator	Describes the users' required action	I want help to @block an IP traffic using the UFW firewall.
@object	Explicitly describes an element to apply the operator	I want to block the @Port 22 using IPtables.

SecBot supports functions that can be run as an action in response to users' inputs, according to an identified *Intent*, such as providing feedback messages, running arbitrary code (*i.e.*, custom actions), or listening for new inputs. Based on that, SecBot implements different custom actions that run actions according to different scenario flows. These custom actions involve *(a)* finding the best solution for a request, *(b)* identifying the type of attack based on symptoms, *(c)* helping during the configurations of in-house protections, and *(d)* calculating metrics related to economic impacts of different cyberattacks.

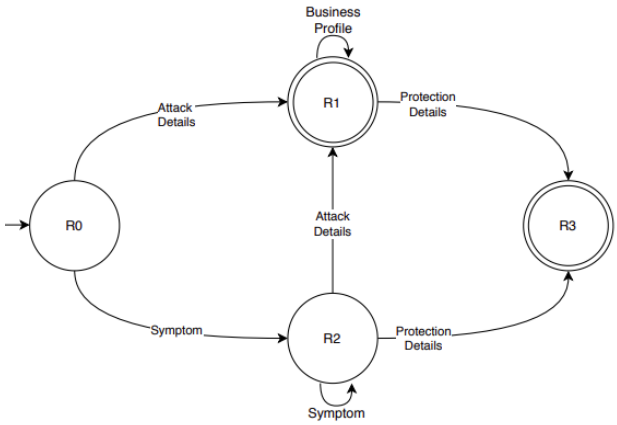
Table 23: Examples of Intents implemented by the SecBot

Intent	Example	Associated Entities
attack_notification	My Windows systems are under a Ransomware attack	@target, @attack_name
attack_details	It is a WannaCry attack	@attack_type
target	The target is my database	@target
problem_desc	My server is receiving a lot of requests from different IPs	@symptom, @target
solution_config	I want to block an SYN flood using my IPTables	@solution, @technology, @target, @attack_name, @action
solution_support	How can I block a specific port using UFW?	@operator, @object, @solution
rosi_calc	Should I invest in backups against Ransomware impacts?	@attack_name
critical_data	I have almost 10 TB of critical data	@cardinal

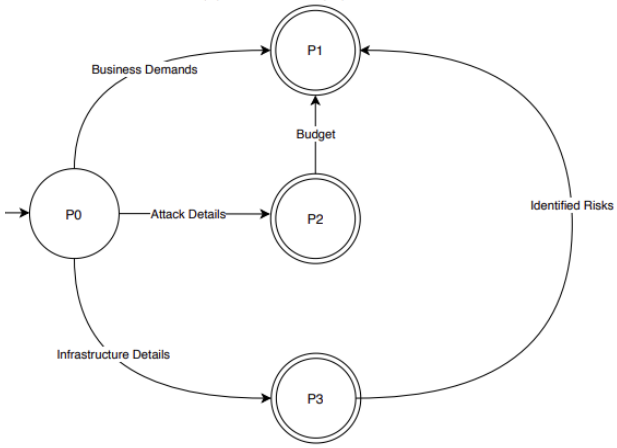
During the training phase of the SecBot, besides database entries and *Intents*, different *Stories* have to be defined for the supervised learning to allow the implemented RASA neural network algorithm to obtain sufficient knowledge to extract and process information. Thus, it is possible to determine which action to take next during a conversation correctly. These *Stories* were defined to cover SecBot scenarios, being able to predict a correct flow based on an identified *Intent*.

5.1.3.1.1. Scenarios

Two approaches are defined to describe different scenarios and to guide users during the interaction with the SecBot: The Reactive (R) and the Proactive (P) approaches. These approaches define, respectively, situations where the user wants to react to protect against an imminent attack or a user that wants to operate a better plan defining the business cybersecurity strategy. These two approaches are divided into six different flows that can be combined to provide a more accurate and complete answer to the user.



(a) Reactive (R) Flow



(b) Proactive (P) Flow

Figure 17: Finite automaton for the SecBot scenarios

Figure 17 (a) describes the finite automaton for **reactive** scenarios. *R1* represents a conversation, where the user knows technical details of the attack (*e.g.*, type of attack or log files) and wants to know which solution matches his/her budget and demands. *R2* focuses on understanding symptoms associated with cyberattacks and problems, thus helping users find a suitable solution. Lastly, the flow resulting in the final state *R3* covers users that already deployed protection solutions but need help to configure these.

The finite automaton for **proactive** scenarios is presented in Figure 17 (b). *P1* assumes users who want to reduce the economic impacts of threats in their business. Different metrics can be employed to provide useful information, directly helping during the decision related to where and when investing in cybersecurity. *E.g.*, the ROSI metric is calculated using the user's inputs and business requirements to provide insights about whether to contract a solution, assume risks, or even acquire a cybersecurity insurance coverage. Furthermore, based on its knowledge database, the agent can suggest actions to reduce costs and to avoid a financial loss for specific business sectors. Scenario *P2* covers the conversation flow in which users want to proactively protect their systems against specific cyberattacks (*e.g.*, WannaCry Ransomware or Mirai Botnet). For that, recommendations for updates, configurations, or solutions to be acquired can be provided. Finally, *P3* considers requests about the most common risks and vulnerabilities according to the business configuration, sector, and information provided.

A business profile descriptor, based on a JSON structure as defined before in the MENTOR's solution, can be configured by users to provide the SecBot with a detailed view about their business. This information is used for the recommendation process and steps requiring specific information on the business organization (*e.g.*, number of employees, regulations, sector, or underlying security configurations/demands). To choose the best solution from a list of possible protections, the SecBot is integrated with MENTOR, a recommendation system for the protection of services introduced also in this report.

Different custom actions are presented next to handle information obtained during the conversation, providing accurate answers for specific cases, where algorithms and calculations are required to process the output, such as those specific reactive and proactive flows described. Custom actions are provided to SecBot to *(a)* identify a cyberattack based on a list of presented problems or symptoms, *(b)* provide configurations for protections according to requests, and *(c)* conduct an economic analysis based on user's requests to support the decision-making.

5.1.3.1.2. Attack Identification

The symptoms or problems extracted from the conversation can be used to identify the attack described by the user. To that end, a decision-tree containing the relationship between known attacks and associated symptoms is proposed as a custom action, which receives a list of symptoms and returns the related attack for the user. This action is directly related to the intent named as *problem_desc* (*cf.* Table 23) which is recognized when the user describes problems without a technical understanding about what is happening.

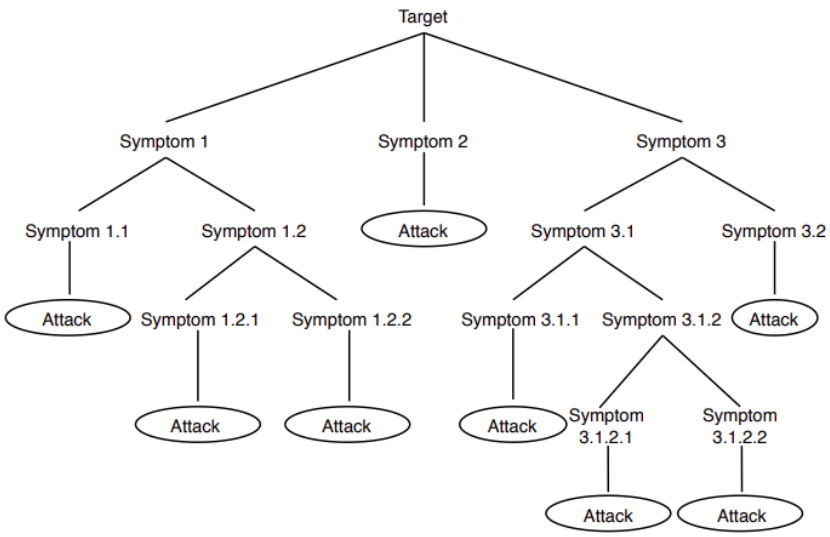


Figure 18: Symptoms' tree structure to search for an attack

Figure 18 shows an example of the attack tree structure. The SecBot starts with an initial tree containing examples of well-known attacks (*e.g.*, Distributed Denial-of-Service - DDoS and ransomware) relationships and their symptoms. Thus, the user's described symptoms are checked in the attack tree. If the resulting path ends in a leaf, it means that the attack was identified. Thus, using a *Server* as a target, the symptoms *"receiving many requests"* and *"many of them are SYN packets"* can result in the identification of an SYN flood attack. The same approach can be applied for different attacks in which previously known

symptoms can be used to create the attack decision-tree. If the path cannot achieve a leaf, it means that the attack cannot be identified, resulting in negative feedback sent to the user.

5.1.3.1.3. Protection Configuration

The SecBot also interprets requests for help to configure protection already available in-house. Hence, entities are extracted to understand *(i)* the intent of the user, which includes the name of the solution available, *(ii)* the operator (*e.g.*, block, allow, or protect), and *(iii)* the attack type for which the user wants a specific configuration. Based on these entities, the SecBot can determine the associated configuration or provide the syntax for the user to create his/her own configuration.

```
<input>: "I have an IPtables installed and I want
    to protect my network against ICMP flood"
Entities_Extraction {
    "intent": solution_configuration
    "solution": IPtables
    "operator": protect
    "target": network
    "attack_name": ICMP flood
}
<custom_action>: find_configuration(solution,
    action, target, attack_name)
<output>: "The command for your configuration
    request is: iptables -t mangle -A PREROUTING -
    p icmp -j DROP"
```

Listing 1: Example of SecBot processing and output based on a user's input

Listing 1 presents the input and output for scenarios where users want to protect the network from an imminent attack (*i.e.*, reactive) or anticipate (*i.e.*, proactive) this type of attack to avoid damages. *E.g.*, the request *"I have an IPtables installed and want to protect my network against ICMP flood"* results in a message containing a configuration for *protection* against *ICMP flood* tailored for the IPTables packet filtering solution. This configuration is provided as a JSON structure stored by the SecBot, which maps different solutions, configurations, and commands.

```
{
  "iptables": {
    "version": "1.4.21",
    "OS": "Linux",
  "support":{
    "block": {
  "ports": "iptables -A INPUT -p <protocol> --
      destination-port <port number> -j DROP",
  "ip traffic": "iptables -A INPUT -s <ip> -j DROP
      "
    }
  },
  "protection_config": {
    "syn flood": "iptables -t raw -A PREROUTING -p
        tcp -m tcp --syn -j CT --notrack |
      iptables -A INPUT -p tcp -m tcp -m
      conntrack --ctstate INVALID,UNTRACKED -j
      SYNPROXY --sack-perm --timestamp --wscale
      7 --mss 1460 | iptables -A INPUT -m
      conntrack --ctstate INVALID -j DROP",
    "icmp flood": "iptables -t mangle -A
      PREROUTING -p icmp -j DROP",
    "port scanning": "iptables -N port-scanning |
      iptables -A port-scanning -p tcp --tcp-
      flags SYN,ACK,FIN,RST RST -m limit --limit
       1/s --limit-burst 2 -j RETURN | iptables
      -A port-scanning -j DROP"
  }
 }
}
```

Listing 2: Example of a JSON file describing a protection configuration

Listing 2 provides an example of this data structure describing a specific solution. In this example, a structure for an IPtables 1.4.21 running on Linux is defined, which supports requests to describe different actions, such as how to block Ports/IP traffic, and also allows for the configuration of IPtables to block different types of attacks (*e.g.*, SYN flood, SSH Bruteforce, and Port Scanning). The Operating System (OS) being used by the business is taken into consideration to provide the correct configuration. This information can be described in the business profile or during the conversation.

5.1.3.1.4. Cybersecurity Investments

The extraction of entities related to the attack (*e.g.*, *@attack_name* and *@attack_type*) and to the business itself (*e.g.*, budget, sector, amount of critical services, and data) is essential for the conversational agent to understand the scenario and to achieve accurate information to calculate the ROSI metric. This metric is defined by Equation 6, where the Reactive Mitigation Cost (RMC) and the total cost (*i.e.*, financial impacts of risk exposure) of a specific attack are calculated given a time-frame T. Furthermore, the Proactive Mitigation Cost (PMC) is used for the ROSI calculation, which defines the cost of investing in approaches or solutions to anticipate threats and avoid future damage (*e.g.*, financial loss). Thus, the higher ROSI is, the more the business is recommended to follow a proactive approach (*e.g.*, to contract backups services or pay for a continuous cloud-based DDoS protection). Otherwise, if ROSI's result is near 0, the business can, *e.g.*, assume risks of economic impacts regarding a possible threat or specific cyberattack.

$$ROSI = \Delta T * \frac{(T_{costs} * RMC) - PMC}{PMC} \qquad (1)$$

Equation 6: ROSI calculation being applied by the SecBot

During the conversation flow, the SecBot can map the attack type based on a specific structure, associating attacks to possible proactive approaches. *E.g.*, for a Ransomware attack, information about the amount of data available (in GB) is required to measure costs of \1 maintaining a full backup to recover from an attack or \2 a cybersecurity insurance. This information is crucial to calculate the ROSI based on this type of attack's possible financial losses. Also, if the user is not able to provide details about specific backup prices for calculation, the SecBot uses an internal database with average costs for different services (*e.g.*, backup, DDoS protection, and anti-phishing) and different attacks (*e.g.*, rescue price for a Ransomware and costs per hour of a DDoS) to provide an approximated ROSI, even with missing inputs from users

5.1.3.2. Evaluation

To evaluate the SecBot, a Proof-of-Concept (PoC) was developed and evaluated using RASA 1.4.6, an open-source machine learning framework to build contextual AI agents and chatbots. SecBot's code and training data set are publicly available. The implemented solution relies on the RASA framework abstractions of the underlying NLP and ML algorithms to simplify the design and handling of Entities and Intents. Custom actions were developed using Python 3.8.3, while the knowledge databases are described as plain text or JSON files. The evaluation was performed using a Dell XPS desktop with the configuration of an Intel Core i7-3770 at 3.40~GHz, 32~GByte of RAM, running a Linux Ubuntu 18.04 LTS 64-bit with the Linux Kernel version 5.3.0-53.

The current training of SecBot is done using a neural network implemented in Rasa to select the next action, which is described as a Long Short-Term Memory (LSTM) architecture. For the training of the neural network, it receives the user's phrase as input and actions as output. During the training phase, it is used as a fitting model with 958 samples (*i.e.*, examples of intents and entities) and a validating split of 0.1 (*i.e.*, 10% of the training dataset as validation data only), which covers 15 different conversation flows with 100% of accuracy for the intent and entities extraction. These results indicate that SecBot can map the conversation for the correct intent available, thus, also being able to extract entities.

In terms of scalability, a stress test revealed that one single instance of SecBot can handle 20 messages per second. Among the currently supported custom actions, a more time-consuming request is the one to identify an attack, using symptoms in the attack tree, which have a computational complexity of *O(n log n)*. In a simulation with an attack tree containing 100 symptoms and 30 attacks (*i.e.*, leaves), the time for the SecBot to process the request and return the correct attack is less than 2~s on average, considering 1,000 repetitions.

5.1.3.2.1. Case Study

The case study was conducted by interacting with an instance of SecBot's prototype running on Telegram, a popular messenger platform. The application interface provided by Telegram simplifies the process of presenting interactions of the business and the SecBot, thus offering a better usability and user-acceptance. However, it is possible to conduct the same case study using the terminal provided by the Rasa framework or even integrating it with other messenger platforms. It is assumed that an SME faces problems in its server infrastructure and wants to find a solution to solve this issue initially, followed by the configuration of on-site protection (*i.e.,* IPtables) and the calculation of ROSI for investments to reduce impacts of a possible ransomware attack.

Users start a chat with the SecBot and ask for help. Symptoms include a server overload with many requests from many different IP addresses, which is initially identified as a DDoS attack. After more symptoms are described and by searching the attack tree (*cf.* Figure 18), the cyberattack is recognized as a DDoS attack characterized by different hosts sending a flood of SYN requests. Based on this information, the user can ask for protection to help against the attack. The user is asked about his/her budget available to invest in protection. Thus, by using details provided in the business profile (*e.g.,* regulations, region, and business sector), the SecBot can select and recommend, from a list of protections against SYN floods, which protection suits best user demands and budget available.

The user continues the conversation for proactively addressing other aspects that can impact the business. This proactive scenario and its interactions see the user asking to support the blocking of port scanning on his/her network. If business protections are not described in the business profile configurations, the SecBot asks whether the user already has a solution installed. In this case, IPtables is available running on the business infrastructure. The SecBot can check in its protection configuration descriptor the correct configuration, and then the proper command is provided for the user to block port scanning. Finally, the user checks with the SecBot about the benefits of investing in backups as a proactive approach to reduce impacts of ransomware attacks, since it can cause all critical business files to be encrypted, requiring rescue for the decryption key. This type of attack typically results in business disruption, financial loss, and also reputation harm. To provide an answer to such a request, the SecBot checks the business profile to understand how much critical data the business has and what the business revenue is. This information is provided in a JSON file used as a descriptor (*i.e.,* business profile) for business configurations and the organization, which can be used as inputs on demand.

The downtime average for the business with similar characteristics (*e.g.,* sector and amount of data) is considered for the analysis, too. Based on all this information, the ROSI (*cf.* Equation 6) is calculated and provided to the user, followed by a final recommendation, which in this case, means that an investment in backups is recommended.

Based on this case study, it is possible to observe the feasibility of the SecBot by providing interactions that cover different flows of the conversation to help in relevant cybersecurity-related tasks. These scenarios encompass the support to react against a cyberattack, configure and manage an existent solution according to the business goals, and obtain information for an efficient cybersecurity planning. Also, the performance of the SecBot is highlighted by answering requests and correctly extracting the information required for these scenarios.

5.1.3.3. Discussion

The SecBot shows opportunities to simplify the different steps involved in cybersecurity management. Challenges to chatbots are also highlighted, since the accuracy achieved by supervised learning methods is directly related to the quality of inputs used. For these scenarios and flows defined, the accuracy of answers provided was precise and useful to address users' demands. The current state, as observed in the PoC implemented, provides directions and shows the benefits of addressing cybersecurity-related information using conversational agents. Custom actions, developed as contributions of this work, indicate the path for further implementations and highlight the proposed solution's extensibility.

Given that the SecBot's prototype has been evaluated by using selected information and scenarios, it is possible to learn new information for handling more requests and conversation flows. There are opportunities to improve the training phase by creating new *Stories* and considering different datasets available for cybersecurity, such as describing more attack characteristics and their relationships. By building a larger dataset of cybersecurity-related information, it is possible to define additional *Entities* to extract from a conversation, thus, resulting in different flows and scenarios covered. In the same way, new *Intents* and scenarios can be defined based on the amount of information that the SecBot can extract. Such *Intents* need to be defined considering the actual demands of businesses, thus resulting in different custom actions to be implemented to address specific requirements.

Information to create the attack decision-tree and configure protections are critical for SecBot. The structure defined is extensible and can cover many more elements and solutions (*e.g.,* configurations for cloud and Network Functions Virtualization-based approaches) according to the knowledge available on its databases. It is crucial to refine and map the actual demands of different sectors regarding the most common types of attacks and their impacts. Also, users can benefit from approaches to simplify the process of deploying recommended solutions, such as by integrating the SecBot with deployment automation mechanisms. Furthermore, for an extensive analysis of vulnerabilities and risk assessment of the business, the SecBot can be integrated with well-known exploits databases for security professionals and researchers (*e.g.,* exploitDB and Rapid7) as well as tools for vulnerability analysis (*e.g.,* Nmap and OpenVAS). This allows non-technical users to interact with the SecBot to gain access to state-of-the-art cybersecurity information and reports about their businesses.

In terms of scalability, several instances of the SecBot can be provided quickly in order to address high demands for interactions. As one instance can handle 20 messages per second, it is reasonable to assume that a single instance of the SecBot can be used by many businesses simultaneously, such as processing more than 100 scenarios (equalling the case study as presented) in one minute. Thus, despite relying on similar underlying data sources, each instance runs independently from the others in a modular fashion via replication. In terms of security, it is an option that each SME can run locally their own instance of the chatbot, which increases the means to operate on dedicated resources in a controlled environment, also allowing to have a knowledge database customized according to the specific demands of that business. It also can scale to complex problems and solutions. However, it depends how to define the correct training data set to use to avoid an over-fitting of the machine learning model being used, *i.e.,* ensuring that the model will be able to extrapolate the knowledge of complex scenarios and not only perform with trained scenarios.

6. Conclusions/ Summary

This deliverable presented an advanced overview of the cybersecurity threat landscape discussed from a technological, legal/policy and economic perspective. The analysis surfaced existing gaps and challenges, described existing practices concerning the "state of play" of cybersecurity within organizations and put forward early recommendations of specific and wider relevance aiming to bridge the gaps identified between the "state of play" and the "state of the art" of cybersecurity. The deliverable took into account the impact of COVID-19, as deemed relevant by each perspective discussed. This document built on the initial analysis of the threat landscape captured under D4.1 (M12); the final analysis of the threat landscape will be captured under D4.3, due in M36. Note that the findings of D4.1, D4.2 and D4. 3 will contribute to CONCORDIA roadmap, due under Task T4.4 in M48. Future work under the three (3) above mentioned perspectives will be shortly discussed below.

6.1 Technical Views

Technological perspective (Chapter 3) focused on two main activities in the 6 domains of interest. First, it refined the threat landscape in D4.1, adding new emerging cybersecurity threats. Second, it analysed and discussed gaps and challenges with respect to identified threats and vulnerabilities, managing crosscutting aspects that affect more domains of interest. Both activities considered the impact of COVID-19 on the cybersecurity threat landscape.

From a technical standpoint, future work will build on activities discussing emerging threats and evolving attacks in D4.1 (Chapter 3), as well as gaps and challenges in D4.2 (Chapter 3). In particular, future work will provide (towards D4.3 due in M36) a set of guidelines, research actions, and an overview of existing countermeasures to address cybersecurity threats, gaps, and challenges. Technical results will also contribute to the overall cybersecurity roadmap envisioned under T4.4.

6.2 Legal Views

The Legal perspective (Chapter 4) encapsulates the developments that have taken place in the regulatory framework relevant to this deliverable since the publishing of D4.1. The Chapter -among other-highlighted the specific provisions of certain legislations that came into play during the COVID-19 pandemic such as the General Data Protection Regulation that deals with processing of health data and the NIS Directive that is applicable to certain sectors including healthcare. Moreover, based -also- on input gathered through interviews conducted -in this year 2, initially - with representatives from the sector-specific CONCORDIA pilots as well as from CONCORDIA's threat intelligence respectively certain certification perspectives, the legal perspective discussed the challenges of the implementation of cybersecurity principles and proposed early-stage recommendations to be refined under Deliverable D4.3. Furthermore, the Legal Perspective expanded on challenges of wider relevance and suggested the way forward.

In terms of future work, as explained earlier (Chapter 4) additional interviews will be conducted within CONCORDIA consortium. More specifically, in 2020 (Year 2), T4.2 focusing on the legal perspective started an initial series of interviews with experts from the

practical and otherwise operational side. Given that the already conducted interviews were with consortium partners, representing industry, in 2021(Year 3) it is anticipated that also other partners representing industry and academia, as well as other members of the CONCORDIA ecosystem both at national and European level will be interviewed in the same manner. Furthermore, regulatory developments that took place as of December 2020 will be, also, discussed under D4.3: 3rd Year Report on Cybersecurity Threats. Overall, the ultimate aim of the legal perspective is to produce well matured recommendations fostering a culture for cybersecurity in a principle based, and future-proof manner

6.3 Economic Views

The work developed within T4.3 introduced new approaches for the risk assessment, planning, and investments in cybersecurity. These approaches will continue to be refined in order to achieve better results to be applied in real-world scenarios. For that, collaborations with CONCORDIA partners are desired. Also, the T4.3 is working also to share the knowledge obtained in a cybersecurity course targeting the cybersecurity consultant profile (as part of contribution for the T3.4). Besides that, research on cybersecurity insurance models are being conducted to identify opportunities and challenges of blockchain for that sector. Further, blockchain-based reputations mechanisms for the cybersecurity providers are under investigation since there are the need to ensure the trust between users and providers in a very competitive market (*i.e.*, cybersecurity solutions).

Regarding the new approaches specifically, the work of T4.3 will continue to: (a) improve and refine SERViz to support new information and scenarios, (b) support new attributes for the customer profile and services in MENTOR, and (c) introduce a solution that integrates all findings of T4.3 in a way to covers the main dimensions of cybersecurity: risk assessment, planning, and deploy of protections. Finally, although the SecBot is motivated by identifying the benefits and challenges of chatbots for SMEs, large companies can also benefit. Professionals with prior knowledge in cybersecurity can explore this approach to meet different goals. Cybersecurity analysts can interact with the SecBot to find a fast and accurate answer for customer requests regarding technical and economic aspects related to SMEs' cybersecurity. Also, mechanisms can be implemented to help large companies justify their investments on a specific solution or cybersecurity strategy, such as understanding requirements to define directions of their bug bounties programs. This can help build foundations for long-term cybersecurity strategies rather than sporadic engagements of specialists.

Overall, in Year 2, activities in T4.1, T4.2, T4.3 have been progressing, as planned. The impact of COVID-19 pandemic has been taken into account in the context the work conducted (e.g. threat landscape). In terms of project implementation, COVID-19 did not affect the activities directly linked to the research and other type of work underlying the present deliverable.

Acronyms

AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threats
BEC	Business Email Compromise
BYOD	Bring-Your-own-Device
CA	Consortium Agreement
CaaS	Cybercrime as a Service
CADA	Continuous Appropriate Dynamic Accountability
CAPEX	Capital Expenditure
CEF	Connecting Europe Facility
CERT-EU	Computer Emergency Response Team
CIA	Certified Information Systems Auditor
CI/CD methodology	Continuous Integration/Continuous Delivery methodology
CISA	Certified Information Systems Auditor
COBOL	Common Business-Oriented Language
CONCORDIA	Cyber security cOmpeteNCe fOr Research anD InnovAtion
COVID-19	Coronavirus Disease 2019
CPU	Central Processing Unit
CRM	Customer Relationship Management
CSA	Cybersecurity Act
CSA	Cloud Security Alliance
CSIRT	Computer Security Incident Response Team
CSIS	Center for Strategic and International Studies
CSPs	Communication Service Provider
CSPs	Cloud Service Providers
CSPCERT	European Cloud Service Provider Certification
CVE	Common Vulnerabilities and Exposures
D	Domain
DBIR	Verizon Data Breach Investigation Report
DDOS	Distributed Denial of Service
DESI	Digital Economic and Society Index
DHCP	Dynamic Host Configuration Protocol
DIET	Dual Intent and Entity Transformer
DNS	Domain Name System
DNS-SEC	Domain Name System Security Extensions
DoA	Description of Action
EC	European Commission
ECCG	European Cybersecurity Certification Group
ECSO	European Cyber Security Organization
EDPB	European Data Protection Board
ENISA	European Union Agency for Cybersecurity
ESISC	European Strategic Intelligence and Security Center
EU	European Union
EUCC	European cybersecurity certification scheme
EUR	Euro
EUROPOL	European Union Agency for Law Enforcement Cooperation
ETL	ENISA Threat Landscape
FISSEA	Federal Information System Security Educators' Association
GA	Grant Agreement
GA	Grant Agreement
GB	Gigabytes
GCSEC	Global Cyber Security Center

GDPR	General Data Protection Regulation
GPSD	General Product Safety Directive
GRC	Governance, risk management and compliance
GTP	GPRS Tunnelling Protocol
HTML	Hyper Text Markup Language document
HTTP	Hyper Text Transfer Protocol
ICMP	Internet Control Message Protocol
ICT	Information Communications Technology
IETF	Internet Engineering Task Force
IIA	Inception Impact Assessment
ID	Identity
IDS	Intrusion Detection Systems
iOCTA	Internet Organised Crime Threat Assessment
IoT	Internet of Things
IP	Internet Protocol address
ISO	International Organization for Standardization
ISP	Internet Service Provider
IT	Information Technology
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
JCU	Joint Cyber Unit
JSON	JavaScript Object Notation
LSTM	Long Short-Term Memory
LTE	Long-Term Evolution
MDR	Medical Device Regulation
ML	Machine Learning
NCSC	National Counterintelligence and Security Center
NFV	Network Functions Virtualization
NIS Directive	Directive on Network and Information Security
NIST	National Institute of Standards and Technology
NLP	Natural Language Processing
OPCW	Organisation for the Prohibition of Chemical Weapons
OPEX	Operational Expenditure
OS	Operating System
OSS	Operation Support System
OWASP	The Open Web Application Security Project
PC	Portable Computer
PLD	Product Liability Directive
PoC	Proof-of-Concept
PMC	Proactive Mitigation Cost
PSDD2	Second Payment Services Directive 2
PSIRT	Products Security Incident Response Team
PPP	Public Private Partnership
PSP	Protection Service Providers
RAM	Random-Access Memory
RDP	Remote Desktop Protocol
RE	Radio Equipment
RED	Radio Equipment Directive
REST	Representational State Transfer
RMC	Reactive Mitigation Cost
RMF	Risk Mitigation Factor
RPC	Remote Procedure Call
ROSI	Return on Security Investment
SDN	Software-Defined Networking
SIGTRAN	Signalling Transport

SIP	Initiation Protocol
SLAs	Service Level Agreements
SME	Small and Medium Enterprises
SMS	Short Message Service
SOC	Security Operation
SOG-IS MRA	Senior Officials Group Information Systems Security Mutual Recognition Agreement
SS	Signalling System
SSH	Secure Socket Shell
SWIPO	Switching Cloud Providers and Porting Data
SYN	Synchronize
T	Threat
TCP	Transmission Control Protocol
TG	Threat Group
TPM	Trusted Platform Module
TV	Television
UAV	Unmanned Aerial Vehicle
UDP	User Datagram Protocol
UK	United Kingdom
UPnP	Universal Plug and Play
US	United States of America
UX	User experiences
VM	Virtual Machine
VPN	Virtual Private Network
VOIP	Voice Over Internet Protocol
VTC	Video-Teleconferencing
VTPM	Virtual Trusted Platform Module
WAF	Web Application Firewall
WMI	Windows Management Instrumentation
WP	Work Package
XPS	eXtreme Performance System

References

[1] C. A. Ardagna, E. Damiani, J. Schutte and P. Stephanow, "A Case for IoT Security Assurance," in *Internet of Things (ITTCC)*, Springer Link, 2017, pp. 175-192.

[2] A. Shaik, R. Borgaonkar, N. Asokan, V. Niemi and J.-P. Seifert, "Practical Attacks Against Privacy and Availability in4G/LTE Mobile Communication Systems," *ArXiv,* vol. abs/1510.07563, 7 August 2015.

[3] S. Hussain, O. Chowdhury, S. Mehnaz and E. Bertino, "LTEInspector: A Systematic Approach forAdversarial Testing of 4G LTE," *Network and Distributed Systems Security (NDSS) Symposium 2018,* February 2018.

[4] M. Chlosta, D. Rupprecht, T. Holz, Pöpper and Christina, "LTE Security Disabled—Misconfiguration inCommercial Networks," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019.

[5] A. Arman, S. Foresti, G. Livraga and P. Samarati, "A Consensus-based Approach for Selecting Cloud Plans," in *2016 IEEE 2nd International Forum on Research and Technologies for Society and Industry Leveraging a better tomorrow (RTSI)*, Bologna, IEEE, 2016, pp. 1-6.

[6] P. K. Rath and G. Anil, "Proposed Challenges and Areas of Concern in Operating System Research and Development," *arXiv preprint arXiv:1205.6423,* 2012.

[7] S. V. Adve and K. Gharachorloo, "Shared Memory Consistency Models: A Tutorial," *IEEEComp,* vol. 29, pp. 66-76, 1996.

[8] G. Boudol and G. Petri, "Relaxed memory models: an operational approach," *ACM SIGPLAN Notices,* vol. 44, pp. 392-403, 2009.

[9] M. F. Atig, A. Bouajjani, S. Burckhardt and M. Musuvathi, "On the verification problem for weak memory models," in *Proceedings of the 37th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages*, New York, 2010, pp. 7-18.

[10] L. Xu, C. Jiang, J. Wang, J. Yuan and Y. Ren, "Information security in big data: privacy and data mining," *Ieee access,* vol. 2, pp. 1149-1176, 2014.

[11] K. Xu, H. Yue, L. Guo, Y. Guo and Y. Fang, "Privacy-preserving machine learning algorithms for big data systems," *2015 IEEE 35th international conference on distributed computing systems,* pp. 318-327, 2015.

[12] Anisetti, Marco; Ardagna, Claudio; Bellandi, Valerio; Cremonini, Marco; Frati, Fulvio; Damiani, Ernesto, "Privacy-aware Big Data Analytics as a service for public health policies in smart cities," *Sustainable cities and society*, vol. 39, pp. 68-77, 2018.

[13] M. Du, K. Wang, Z. Xia and Y. Zhang, "Differential privacy preserving of training model in wireless big data with edge computing," *IEEE Transactions on Big Data,* 2018.

[14] S. Bleikertz, S. Bugiel, H. Ideler, S. Nurnberger and A.-R. Sadeghi, "Client-controlled cryptography-as-a-service in the cloud," *International Conference on Applied Cryptography and Network Security*, pp. 19-36, 2013.

[15] I.-L. Yen, F. Bastani, N. Solanki, Y. Huang and S.-Y. Hwang, "Trustworthy Computing in the Dynamic IoT Cloud," *2018 IEEE International Conference on Information Reuse and Integration (IRI)*, pp. 411-418, 2018.

[16] C. A. Ardagna, E. Damiani, J. Schutte and P. Stephanow, "A case for IoT security assurance," in *Internet of Everything*, Springer, 2018, pp. 175-192.

[17] S. Taherizadeh, A. C. Jones, I. Taylor, Z. Zhao and V. Stankovski, "Monitoring self-adaptive applications within edge computing frameworks: A state-of-the-art review," *Journal of Systems and Software,* vol. 136, pp. 19-38, 2018.

[18] M. Ambrosin, M. Conti, A. Ibrahim, A.-R. Sadeghi and M. Schunter, "SCIoT: A Secure and sCalable End-to-End Management Framework for IoT Devices," in *European Symposium on Research in Computer Security*, Springer, 2018, pp. 595-617.

[19] R. Rani, S. Kumar and U. Dohare, "Trust Evaluation for Light Weight Security in Sensor Enabled Internet of Things: Game Theory Oriented Approach," *IEEE Internet of Things Journal,* vol. 6, no. 5, pp. 8421-8432, 2019.

[20] R. Binns, "Fairness in Machine Learning: Lessons from Political Philosophy," in *Conference on Fairness, Accountability and Transparency*, PMLR, 2018, pp. 149-159.

[21] R. Jung, J.-H. Jourdan, R. Krebbers and D. Dreyer, "RustBelt: Securing the Foundations of the Rust Programming Language," *Proceedings of the ACM on Programming Languages,* vol. 2, pp. 1-34, 2017.

[22] A. A. U. Rahman and L. Williams, "Software Security in DevOps: Synthesizing Practitioners' Perceptions and Practices," in *2016 IEEE/ACM International Workshop on Continuous Software Evolution and Delivery (CSED)*, IEEE, 2016, pp. 70-76.

[23] L. Bass, R. Holz, P. Rimba, A. B. Tran and L. Zhu, "Securing a Deployment Pipeline," in *2015 IEEE/ACM 3rd International Workshop on Release Engineering*, IEEE, 2015, pp. 4-7.

[24] M. Evans, L. Maglaras, Y. He and H. Janicke, "Human Behaviour as an aspect of Cyber Security Assurance," *Security and Communication Networks 9(17),* 2016.

[25] T. Holz, N. Pohlmann, E. Bodden, M. Smith and J. Hoffmann, "Human-Centered. Systems Security," Bochum, 2016.

[26] I. Corradini and E. Nardelli, "Building Organizational Risk Culture in Cyber Security: The Role of Human Factors," in *Advances in Human Factors in Cybersecurity*, vol. 782, Springer, Cham, 2019.

[27] N. Sohrabi Safa, R. Von Solms and L. Futcher, "Human aspects of information security in organisations," *Computer Fraud & Security,* pp. 15-18, 2016.

[28] A. Vieane, G. Funke, R. Gutzwiller, V. Mancuso, B. Sawyer and C. Wickens, "Addressing Human Factors Gaps in Cyber Defense," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 2016.

[29] A. Rashid, G. Danezis, H. Chivers, E. Lupu, A. Martin, M. Lewis and C. Peersman, "Scoping the Cyber Security Body of Knowledge," *IEEE Security & Privacy,* vol. 16, no. 3, pp. 96-102, 2018.

[30] H. Aldawood and G. Skinner, "Challenges of Implementing Training and Awareness Programs Targeting Cyber Security Social Engineering," in *2019 Cybersecurity and Cyberforensics Conference (CCC)*, May 2019.

[31] M. Courtney, "States of cyber-warfare," *Engineering & Technology,* vol. 12, no. 3, pp. 22-25, 2017.

[32] R. Hughes, "NATO and Cyber Defence," in *Atlantisch Perspectief,* 2009, p. 33.

[33] C. S. Yoo, "Cyber Espionage or Cyberwar?: International Law, Domestic Law, and Self-Protective Measures," in *Cyberwar: Law and Ethics for Virtual Conflicts,* 2015, pp. 15-3.

[34] C. Everett, "The lucrative world of cyber-espionage," *Computer Fraud & Security,* vol. 7, pp. 5-7, 2009.

[35] B. Watkins, "The impact of cyber attacks on the private sector," Association for International Affair, 2014.

[36] M. Bressler and L. Bressler, "Protecting your company's intellectual property assets from cyber-espionage," *Journal of Legal, Ethical, and Regulatory Issues,* vol. 18, no. 1, p. 21, 2015.

[37] A. Garg, J. Curtis and H. Halper, "Quantifying the financial impact of IT security breaches," *Information Manaement & Computer Security,* vol. 11, no. 2, pp. 73-84, 2003.

[38] E. Gal-Or and A. Ghose, "The Economic Consequences of Sharing Security Information," in *Economics of information security,* Boston, MA, 2004.

[39] S. Chai, M. Kim and H. Rao, "Firms' information security investment decisions: Stock market evidence of investors' behavior," *Decision Support Systems,* vol. 50, no. 4, pp. 651-661, 2011.

[40] L. Gordon, M. Loeb and L. Zhou, "The Impact of Information Security Breaches: Has There Been a Downward Shift in Costs?," *Journal of Computer Security,* vol. 19, no. 1, pp. 33-56, 2011.

[41] V. Richardson, M. W. Watson and R. E. Smith, "Much Ado about Nothing: The (Lack of) Economic Impact of Data Privacy Breaches," *Journal of Information Systems,* 2019.

[42] Z. He, T. Frost and R. Pinsker, "The Impact of Reported Cybersecurity Breaches on Firm Innovation," *Journal of Information Systems,* 2019.

[43] P. Rosati, M. Cummins, P. Deeney, F. Gogolin, L. Van der Werff and T. G. Lynn, "The effect of data breach announcements beyond the stock price: Empirical evidence on market activity," *International Review of Financial Analysis,* vol. 49, pp. 146-154, 2017.

[44] C. Scherer and H. Cho, "A Social Network Contagion Theory of Risk Perception," *Risk analysis : an official publication of the Society for Risk Analysis,* vol. 23, no. 2, pp. 261-267, 2003.

[45] V. Bakir, "Media and risk: Old and new research directions," *Journal of Risk Research,* vol. 13, no. 1, pp. 5-18, 2010.

[46] I. Chung, "Social Amplification of Risk in the Internet Environment," *Risk analysis : an official publication of the Society for Risk Analysis,* vol. 31, no. 12, pp. 1883-1896, 2011.

[47] W. Gharibi and M. Shaabi, "Cyber Threats In Social Networking Websites," *International Journal of Distributed and Parallel Systems,* vol. 3, 2012.

[48] J. a. Z. P. a. J. Y. Gao, H. Chen, Y. Mao, S. Chen, Y. Wang, H. Fu and J. Dai, "Mental health problems and social media exposure during COVID-19 outbreak," *Plos one,* vol. 15, no. 4, p. e0231924, 2020.

[49] Y. Huang and N. Zhao, "Generalized anxiety disorder, depressive symptoms and sleep quality during COVID-19 outbreak in China: a web-based cross-sectional survey," *Psychiatry research,* p. 112954, 2020.

[50] Capgemini Invent, European Digital SME Alliance, and Executive Agency for Small and Medium-sized Enterprises (European Commission), Technopolis, "Skills for SMEs: Cybersecurity, Internet of things and Big Data for Small and Medium-sized Enterprise," 2019.

[51] Proofpoint, "User Risk Report: Exploring Vulnerability and Behaviour in a People-Centric Threat Landscape," Proofpoint Annual Report, 2020.

[52] M. Pappalardo, M. Niemiec, M. Bozhilova, N. D. A. Stoianov 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.

[53] B. Rodrigues, M. Franco, G. Parangi and B. Stiller, "SEConomy: a Framework for the Economic Assessment of Cybersecurity," in *Economics of Grids, Clouds, Systems, and Services*, Leeds, Springer LCNS, 2019, pp. 154-166.

[54] C. Inan, M. Franco, B. Rodrigues and B. Stiller, *A Visual Tool for the Analysis of Cybersecurity Investments*, Zurich: University of Zurich, 2020.

[55] M. Franco, B. Rodrigues and B. Stiller, "MENTOR: The Design and Evaluation of a Protection Services Recommender Systems," in *15th International Conference on Network and Service Management (CNSM)*, Halifax, Canada, 2019.

[56] European Union Agency for Network and Information Security (ENISA), "Information Security and Privacy Standards for SMEs," 2016.

[57] M. Franco, B. Rodrigues, E. Scheid, A. Jacobs, L. Granville and B. Stiller, "SecBot: a Business-Driven Conversational Agent for Cybersecurity Planning and Management," in *International Conference on Network and Services Management (CNSM)*, Izmir, Turkey, 2020.

[58] T. Bunk, D. Varshneya, V. Vlasov and A. Nichol, *DIET: Lighweight Language Understanding for Dialogue Systems*, Arxiv, 2020.

[59] Rasa Technologies, *Rasa: Open Source Conversational AI*, 2020.