Grant Agreement No.: 101096342
Call: HORIZON-JU-SNS-2022
Topic: HORIZON-JU-SNS-2022-STREAM-B-01-04
Type of action: HORIZON-JU-RIA

Holistic, omnipresent, resilient services
for future 6G wireless and computing ecosystems

D6.2 Impact Creation Report and Exploitation Strategy

Revision: v.1.0

Work package	WP6
Task	Task 6.1, 6.2, 6.3
Due date	30/06/2024
Submission date	01/07/2024
Deliverable lead	Martel Innovate
Version	1.0
Authors	Amrita Prasad (Martel Innovate), Niikolaos Androulidakis (8Bells), Michael Danousis (8Bells), Diego Lopez (Telefonica)
Reviewers	Fabrizio Granelli (CNIT)

Abstract	This deliverable describes the communication, dissemination, standardization, and exploitation activities, conducted in the first half of project (January 2023 – June 2024) to guarantee broad and effective visibility, promotion and continuity of the project's work and outcomes.

Keywords	Dissemination, Communication, Exploitation, Standardization, Press, Outreach, Liaisons, Events, KPIs, KERs

DOCUMENT REVISION HISTORY

Version	Date	Description of change	List of contributor(s)
V0.1	23/04/2024	Table of content	Amrita Prasad (Martel Innovate)
V0.2	14/06/2024	Exploitation strategy draft ready	Alexandros Dimos (8Bells)
V0.3	19/06/2024	Impact creation report draft ready	Amrita Prasad (Martel Innovate)
V0.4	25/06/2024	Standardization report draft ready	Diego Lopez (Telefonica)
V0.5	28/06/2024	Internal review	Fabrizio Granelli (CNIT)
V0.6	30/06/2024	Addressing of comments	Alexandros Dimos (8Bells)
V0.7	30/06/2024	Addressing of comments	Amrita Prasad (Martel Innovate)
V1.0	01/07/2024	Final fixing	Miguel Alarcon (Martel Innovate)
V1.1	18/11/2024	Review of the chapters 7, 8 and 9 according to reviewer's comments	Nikolaos Androulidakis (8Bells), Michael Danousis (8Bells)
V1.2	25/11/2024	Updates in SWOT analysis and KER exploitation pathways	Nikolaos Androulidakis (8Bells), Michael Danousis (8Bells)
V1.3	28/11/2024	Updated on individual exploitation plans	Nikolaos Androulidakis (8Bells), Michael Danousis (8Bells)
V1.4	11/12/2024	Finalisation on market analysis	Nikolaos Androulidakis (8Bells), Michael Danousis (8Bells)

Disclaimer

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the other granting authorities. Neither the European Union nor the granting authority can be held responsible for them. This work has received funding from the Swiss State Secretariat for Education, Research and Innovation (SERI).

Copyright notice

Project co-funded by the European Commission in the Horizon Europe Programme	
Nature of the deliverable:	**R***

Dissemination Level		
PU	*Public, fully open, e.g. web*	**x**
SEN	*Sensitive, limited under the conditions of the Grant Agreement*	
Classified R-UE/ EU-R	*EU RESTRICTED under the Commission Decision No2015/ 444*	
Classified C-UE/ EU-C	*EU CONFIDENTIAL under the Commission Decision No2015/ 444*	
Classified S-UE/ EU-S	*EU SECRET under the Commission Decision No2015/ 444*	

* *R: Document, report (excluding the periodic and final reports)*
DEM: Demonstrator, pilot, prototype, plan designs
DEC: Websites, patents filing, press & media actions, videos, etc.
DATA: Data sets, microdata, etc
DMP: Data management plan
ETHICS: Deliverables related to ethics issues.
SECURITY: Deliverables related to security issues
OTHER: Software, technical diagram, algorithms, models, etc.

Executive summary

The document at hand, developed in the context of WP6, builds upon what has been outlined in D6.1 (Impact Creation Strategy and Plan); the document serves the main purpose of offering an in-depth report on the project's communication, dissemination, and community-building strategy that has been developed in the first half of the project. The strategy has been followed by all project partners to maximize the impact of HORSE project and ensure that the following communication-related project objectives are met:

- Ensure HORSE's broad visibility by spreading knowledge about project activities and its results.
- Reach, stimulate, and engage a critical mass of relevant stakeholders to ensure that the project results are effectively showcased, leading to widespread validation, improvement, and further adoption of the developed technologies and concepts.
- Facilitate exploitation of project outcomes and promote the development of innovative solutions based on the HORSE technologies and architecture.
- Foster an impactful contribution to relevant standardization bodies.
- Ensure close coordination with the SNS community and establish liaisons with relevant initiatives, such as 6G-IA, SNS-JU, etc.

Beside describing the communication, dissemination, and community-building activities conducted by the HORSE consortium during M01-M18 of the project, D6.2 presents actions taken to address recommendations offered during the previous project review, plans of activities after the project's end, and offers an overview on standardization and exploitation plans developed by project partners.

Table of contents

List of figures

List of tables

Abbreviations

5G	5th Generation
6G	6th Generation
6G IA	6th Generation Industry Association
AI	Artificial Intelligence
B5G	Beyond 5G
CAGR	Compound Annual Growth Rate
CFP	Call for Papers
CSA	Coordination and Support Action
DDoS	Distributed Denial of Service
DT	Digital Twin
ER	Exploitable Result
GDPR	General Data Protection Regulation
GenAI	Generative AI
IDR	Intrusion Detection and Response
IoE	Internet of Everything
IoT	Internet of Things
IP	Internet Protocol
KER	Key Exploitable Result
KPI	Key Performance Indicator
M	Month
M2M	Machine to Machine
ML	Machine Learning
MNO	Mobile Network Operator
NDT	Network Digital Twin
NLP	Natural Language Processing
PQC	Post-Quantum Cryptography
Q1	Quarter 1
R&I	Research and Innovation
RIA	Research and Innovation Action
SaaS	Software-as-a-Service

SNS	**Smart Network and Services**
SNS JU	**Smart Network and Services Joint Undertaking**
TCP	**Transmission Control Protocol**
vRAN	**virtual Radio Access Network**
WP	**Work Package**
XR	**Extended Reality**

1 INTRODUCTION

During the period from M1 to M18 of the project, WP6 was dedicated to implementing an extensive range of tools and initiatives to initially disseminate information and engage with relevant stakeholders. WP6 worked in close collaboration with other WPs in the HORSE project, the SNS JU, the European Commission, and other pertinent SNS projects.

1.1 Purpose of the document

The Impact Creation Report and Exploitation Strategy for the reporting period (Jan 2023 – June 2024) presents an overview of the communication and dissemination activities of the HORSE project. This deliverable expands upon the strategic framework established in Deliverable 6.1, "Impact Creation Strategy and Plan" and aims to achieve the following objectives:

- Describe the implemented communication and engagement activities, as well as the monitoring and evaluation processes.
- Illustrate how the methods, tools, and promotional materials have been utilized in the project's dissemination and communication efforts
- Provide a comprehensive summary of the communication activities. The report focuses on the key actions carried out during the initial communication phase of the project. This phase aimed to proactively engage target stakeholders, generate interest in HORSE's activities and outcomes, and establish a robust foundation for the planned dissemination activities.

1.2 Structure of the document

This deliverable flows as 1 document but there are input and updates from all 3 tasks of the WP6, which are updates on the communication and dissemination activities for impact creation, a report on the standardization activities and finally an exploitation plan for the HORSE tools and technologies. Therefore, the document reads first the impact creation update, then the exploitation plan and finally an update on the standardization activities.

2 Communication and Dissemination

Communication and dissemination activities are central to the overall HORSE effort. They are being closely monitored and coordinated to ensure an effective engagement of all targeted stakeholders, including those in the broader 6G, privacy and cybersecurity ecosystems and related vertical domains. To raise awareness and maximize the impact of the project, a comprehensive communication and dissemination plan has been developed in Q1 of the project (see D6.1 for details). Its execution began at the early project stages and continued at steady pace throughout its whole duration. Building upon the activities outlined in the Impact Creation Strategy and Plan (D6.1) - a set of dedicated online and offline activities, outlined below, has been pursued to support the achievement of project objectives and ensure a broad promotion and effective showcasing of developed concepts, technologies, use cases, and project results. These activities are conducted under MARTEL's leadership and guidance with active contributions from all HORSE project partners.

WP6 leads a set of dedicated dissemination and communication actions with the following objectives:

- Ensure broad visibility and awareness of HORSE, promoting project knowledge and establishing a recognizable identity to support promotional and marketing efforts.
- Engage and stimulate a critical mass of relevant stakeholders to effectively showcase project results, leading to validation and further adoption of the developed technologies.
- Contribute significantly to relevant scientific domains and standardization bodies as appropriate and relevant to planned exploitation plans and project outcomes.
- Establish liaisons and ensure close collaboration with relevant initiatives in the industry and R&I domains, particularly those launched as a result of the SNS joint undertaking, other similar initiatives, and projects being funded in the SNS stream B.

Communication and Dissemination phases

In the reporting period, dissemination and communication activities were carried out related to the first and second phase of communication and dissemination activities, as defined in D6.1: Impact Creation Strategy and Plan according to Figure 1.

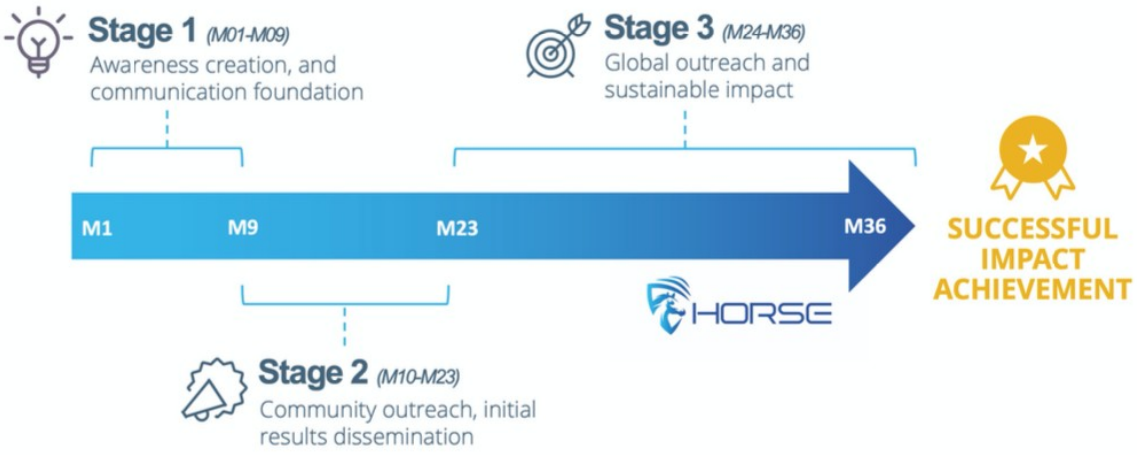


Figure 1: HORSE Impact Creation phases

During the first and the second phase, the primary focus was on engaging target stakeholders and present the result of the project. dissemination activities. The following communication strategy and activities were carried out:

- Organizing the first workshop: HORSE project organized a workshop in collaboration with WP2 in M4 of the project in order to generate the use-case requirements
- Presenting project results: HORSE showcased the initial outcomes and milestones at various events and conferences.
- Producing videos to raise awareness: These promotional video were created to highlight the project's objectives, achievements, and impact.
- Animating social media channels: The project team actively engaged with stakeholders and the public through various social media platforms.
- Publishing news items on the project website and media: Regular updates were posted to keep stakeholders informed about the project's progress.
- Distributing newsletters: Periodic newsletters were sent out to stakeholders to maintain interest and update them on project milestones.
- Participating in events: Team members attended events to network, share knowledge, and promote the project.

2.1 Communication and dissemination activities M1-M18

2.1.1 Project website

The HORSE website **www.horse-6g.eu** (see Figure 2), has been developed to act as an information hub presenting the project's goals, activities, and achievements. The website was launched in January 2023 at the time of the official start of the project and features the following:

- General information about the project, its vision, objectives, and anticipated impact.
- Information about project use cases and enabling functions.
- A brief introduction to all members of the consortium.
- News items and press releases.
- List of relevant events.
- A repository of resources, such as scientific publications, presentations/talks, promotional materials, videos, and public deliverables.
- Contact forms and information.
- An acknowledgment and reference to the Smart Networks and Services Joint Undertaking of the European Union's Horizon Europe Research and Innovation programme.

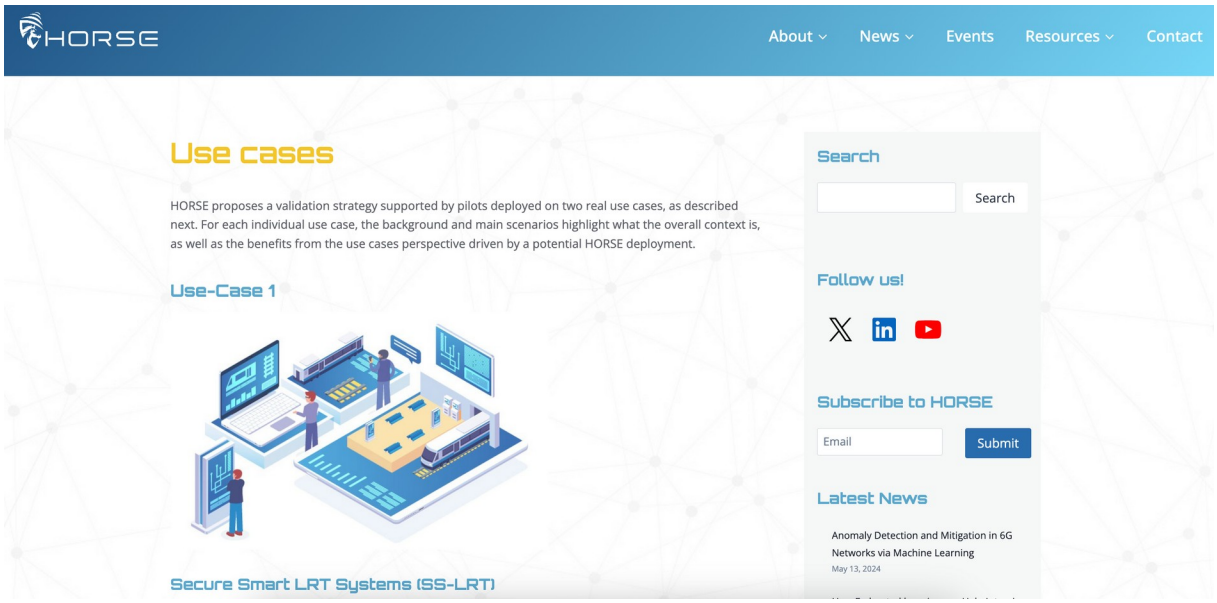


Figure 2: HORSE website

The website is being periodically updated according to the evolution of the project.

In terms of reach/engagement, in the reporting period, the website counts **3917 unique visitors**, that have generated **7472 page views** and an average visit duration of about 2mins as shown in Figure 3.

Figure 3: HORSE website statistics

The most viewed pages of the website are (see Figure 4):

Pages

PAGE URL	PAGEVIEWS	▼ UNIQUE PAGEVIEWS
/index	3,756	3,235
consortium	529	452
latest-news	459	357
use-cases	292	266
deliverables	256	236
horse-tools	223	207
all-events	224	181
presentations	179	161
contact	132	111
publications	116	111
promo-materials	101	90
event	116	88
videos	104	87

Figure 4: Page views on HORSE website

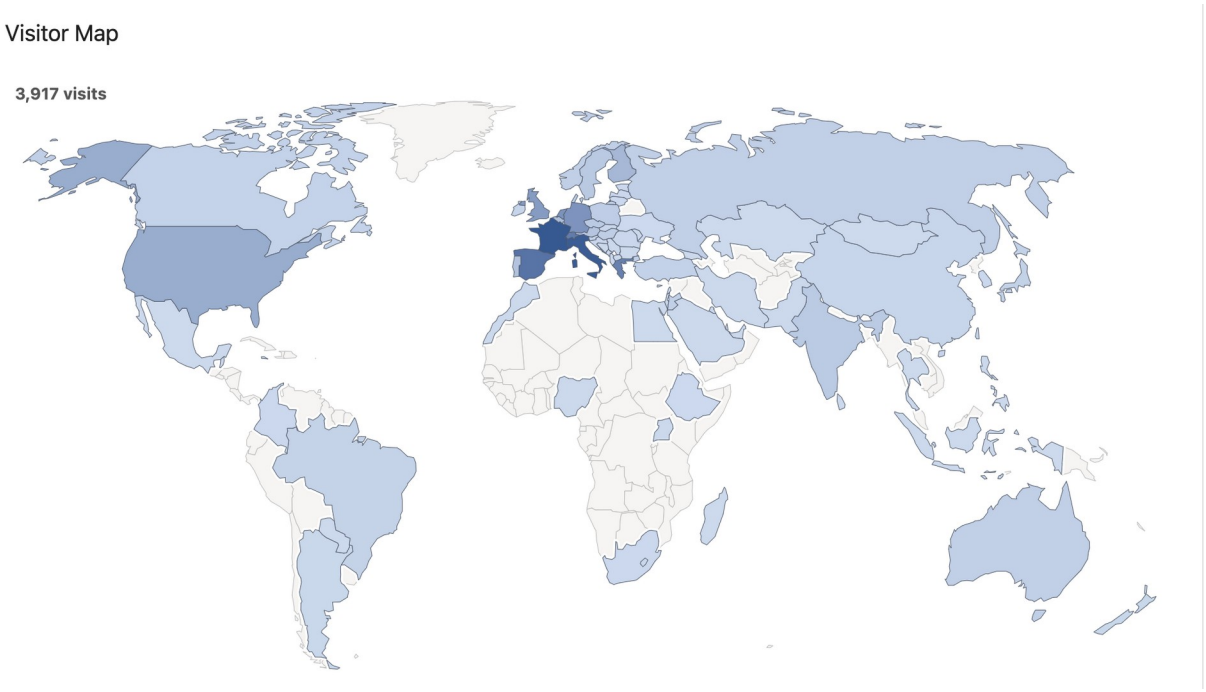


Figure 5: Geographical distribution of the visitors of the HORSE website

The most visits, seen in Figure 5, are from France, Italy, Spain, Switzerland and Greece. This reflects, in part, the composition of the consortium and the communication activities undertaken by partners.

Based on the provided analytics data for the HORSE website for the period of **Jan 2023 to Jun 2024**, we have the following traffic sources:

- **Organic Search: 1988 visits (51%)** : Organic search traffic refers to users who found website through a search engine (e.g., Google, Bing, Yahoo) by entering relevant keywords.
- **Direct: 1527 visits (39%):** Direct traffic occurs when users type the website's URL directly into their browser's address bar, access it through browser bookmarks, or click on a link in an email or a document (e.g., a PDF). This traffic source often reflects users who are already familiar with the project or have visited the website before.
- **Referral: 221 visits (5.6%)** : Referral traffic is generated when users visited the website by clicking on a link from another website. This can include links in blog posts, news articles, or online directories.
- **Social: 181 visits (4.6%):** Social traffic comes from users who find and visit the website through social media platforms (e.g., Facebook, Twitter, LinkedIn, Instagram).

Measures to improve website traffic:

Enhance Organic Search Traffic: Organic search accounts for 51% of the total traffic, indicating that there is significant room for improvement. To boost organic search traffic, we will focus on:

- Conducting thorough keyword research and incorporating relevant keywords into the website's content.
- Improving on-page SEO by optimizing metadata (title tags, meta descriptions, header tags, etc.) and creating high-quality, informative content that engages visitors.
- Utilizing internal and external links to improve site navigation and build a strong backlink profile.
- Regularly updating and maintaining the website to ensure optimal performance and user experience.

Strengthen Social Media Presence: Social media contributes 4.6% of the total traffic, indicating potential growth in this area. To increase social traffic, we will consider:

- Developing a consistent and engaging social media strategy that includes regular content updates, audience engagement, and promotion of the website.
- Leveraging various social media platforms such as Twitter and LinkedIn to reach a wider audience.
- Creating shareable content (e.g., blog posts, infographics, videos) to encourage our audience to share your content on their social media profiles.

Boost Referral Traffic: With referrals accounting for 5.6% of the total traffic, there's room to increase this metric. To enhance referral traffic, we will consider:

- Establishing partnerships with relevant industry websites, blogs, or online communities.
- Engaging in guest posting on authoritative websites in HORSE's niche.
- Offering valuable resources, such as whitepapers or webinars, that can be shared by other websites.

Direct Traffic: Direct traffic constitutes 39% of website's traffic. It is important to understand the source of this traffic and identify potential growth opportunities. We will consider:

- Ensuring that the website is easily accessible through clear navigation, fast loading times, and mobile-friendly design.
- Encouraging repeat visitors by offering valuable content.

By focusing on these recommendations, we can work towards a more balanced traffic acquisition strategy and increase the overall performance of the HORSE website.

All information and e-mails collected are protected under the General Data Protection Regulation (GDPR). Contact is and will continue to only be made with people who have submitted inquiries. Similarly, the newsletters are and will continue to be sent out only to individuals who have explicitly requested to receive them. Any person who has subscribed can request for their e-mail address to be removed from the list. The website provides information on the data kept and how they are used in alignment with the GDPR under the Privacy policy link (footer of the webpage).

Last but not the least, HORSE opted for an environmentally responsible website hosting platform, which has been designed to be as energy efficient as possible to limit the unnecessary waste of resources. The web hosting provider, GreenGeeks, puts back three times the power consumed into the grid in the form of renewable energy.

2.1.2 Social media channels

HORSE established its presence on social media channels to regularly promote project activities and outputs while encouraging a wider discussion on topics related to 6G research and deployment as well as topics like AI/ML, cybersecurity, privacy, digital twinning etc. The project has built a fair follower base on the prominent social media channels, namely X/Twitter and LinkedIn which are all linked to the project's website.

For most of the promotional posts, social media cards are created following the brand identity of the project and these social media cards are used for the promotion of project events, international days of relevance, newsletter announcements etc. Some example of social media cards produced for HORSE project are:

Figure 6: HORSE project social media cards

2.1.2.1 X (Former Twitter)

HORSE uses X/Twitter, as it is a very dynamic social network covering the news in real-time at a global level. To date, the HORSE Twitter account (@HORSEProjectEU) has attracted **251 followers**. The project follows 133 accounts, mostly projects and initiatives in similar fields. The project's X account is used predominately to promote and disseminate project activities and developments but also to learn about and cross-share relevant and interesting events and initiatives, and to establish meaningful connections with relevant stakeholders, including policy makers, industry, and the general public.

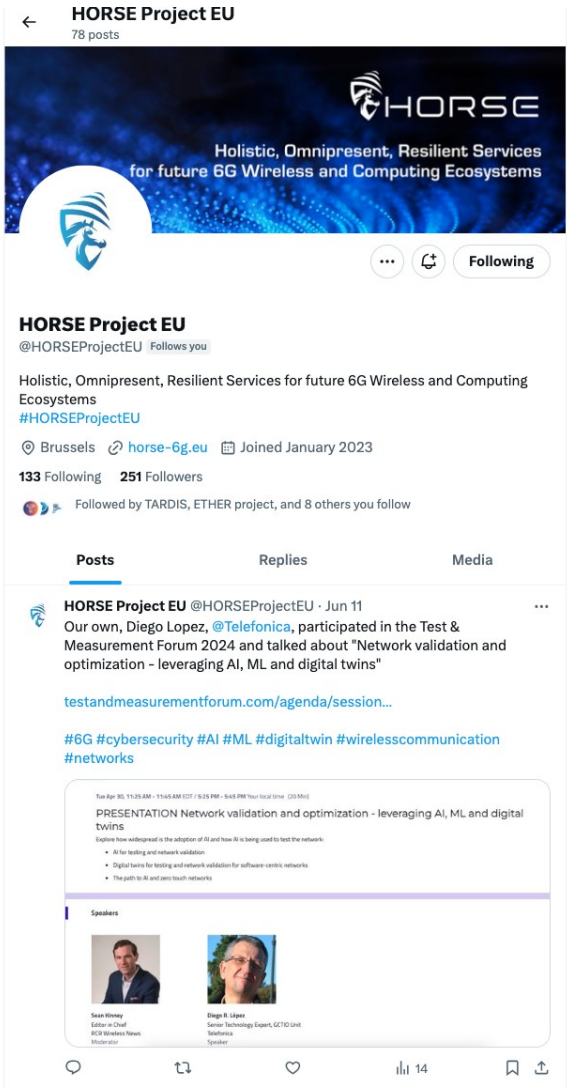


Figure 7: HORSE project X account

2.1.2.2 LinkedIn

LinkedIn, as one of the biggest business networks in the world (over 150 million users in more than 200 countries and territories), is a useful tool for HORSE. It allows the project to network with individuals and organizations within the industry and beyond, share relevant information about project activities, and stay up to date on the latest developments in the field. To date, the HORSE LinkedIn account (horse-project-eu) has attracted **361 followers**. Similar to X, the LinkedIn account is used to promote project activities and learn about and cross-share relevant events and activities. Figure 8 presents the project's LinkedIn profile.

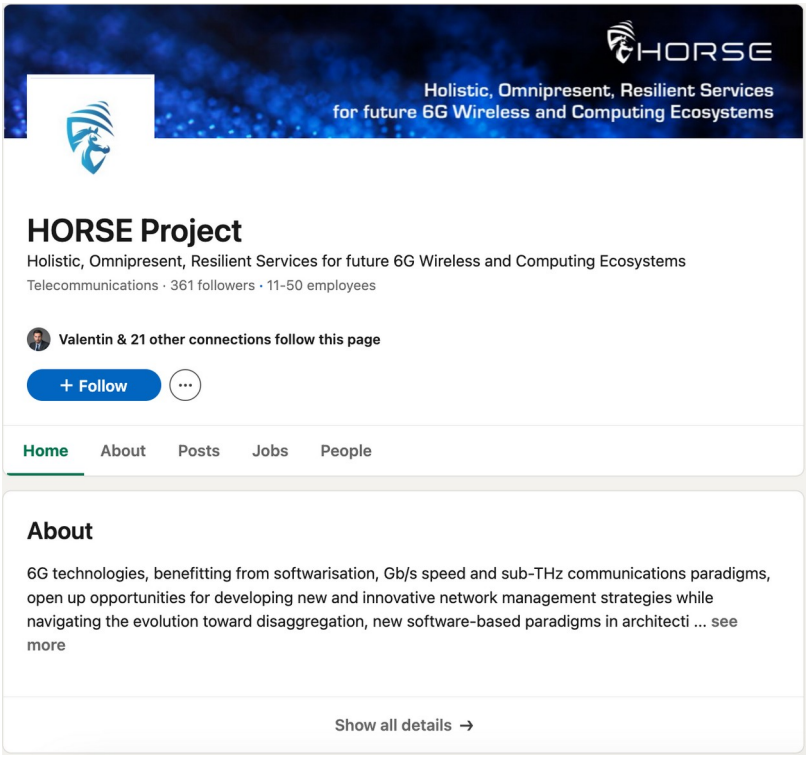


Figure 8: HORSE LinkedIn Page

2.1.3 News items, press releases

The HORSE consortium keeps the community and the general public informed about relevant activities, undertakings, and events by publishing news items and press releases. To date, 12 news items and 1 press release have been published on the project website.

The consortium has an effective way of generating technical content from the project. The consortium produces a blogpost per month which a partner has to provide. The idea of the blogpost is about a technical in depth writeup about a technology or a concept that is useful to the HORSE and 6G community. So far 5 technical blogposts have been published from the consortium.

Figure 9 shows the news items and blogposts published on the website.

Figure 9: Published news items and blogposts

2.1.4 Newsletters

The HORSE periodic newsletter is sent out twice a year, providing updates on the 6G, privacy and cybersecurity ecosystems, as well as on the project activities, findings, and results. The project newsletters also contain information on the upcoming tasks, events, as well as any relevant news and announcements from individual project partners when relevant. A mailing list based on subscription has been created, giving the possibility to share the newsletter via mass mailing. A registration functionality allowing interested visitors to subscribe to the newsletter has been available on the project website since the beginning of the project. The design of each newsletter is aligned with the HORSE brand identity. The newsletter is also fully responsive to ensure its readability on any device.

All issued newsletters are being uploaded on the website upon their distribution to subscribers. To date, 2 newsletters have been sent out (see Figure 10), the 3rd edition is planned for June 2024.

Figure 10: HORSE published newsletters

2.1.5 Publications

The HORSE consortium is committed to bringing research results closer to the public and adheres to the Open Access guidelines set by the Horizon Europe work programme. All project partners are strong supporters of Open Access as it enables all interested parties to use published research results irrespectively of their location or income, boosting the transfer of knowledge between science, the economy, and society at large. The project has been very

active in that sphere since its early stages. The below Table 1 lists all the accepted/published papers stemming from HORSE in the reporting period.

Table 1: HORSE scientific publications

Title of the paper	Authors	Conference/Journal
Optimum Network Slicing for Ultra-reliable Low Latency Communication (URLLC) Services in Campus Networks	Iulisloi Zacarias and Francisco Carpio and André Costa Drummond and Admela Jukan	2023 19th International Conference on the Design of Reliable Communication Networks (DRCN)
Smart Control of Mission Critical Services in beyond 5G Networks: Architecture, Deployment Options, and Experimental Results (under review R2)	Sotirios Spantideas, A. Giannopoulos, P. Koufou and P. Trakadas	IEEE Transactions on Machine Learning in Communications and Networking
Improving Connectivity in 6G Maritime Communication Networks with UAV Swarms	Nikolaos Nomikos, Anastasios Giannopoulos, Alexandros Kalafatelis, Volkan Ozduran, Panagiotis Trakadas, George K Karagiannidis	IEEE Access
Relay-Aided Uplink NOMA Under	Volkan Ozduran, Nikolaos Nomikos, Ehsan Soleimani-Nasab, Imran Shafique Ansari, Panagiotis Trakadas	IEEE Open Journal of Vehicular Technology
On the Performance of Uplink Power-Domain	Volkan Ozduran, Mohammadali Mohammadi, Nikolaos Nomikos, Imran Shafique Ansari, Panagiotis Trakadas	IEEE Access
A Packet Delay Emulator for High-Bandwidth andLow-Latency Traffic in 5G Networks	Raffaele Bolla, Roberto Bruschi, Franco Davoli, Chiara Lombardo,Alireza Mohammadpour, Ramin Rabbani	IEEE Globecom 2023
Leveraging Network Data Analytics Function and Machine Learning for Data Collection, Resource Optimization, Security and Privacy in 6G Networks	P. Gkonis, N. Nomikos, P. Trakadas, L. Sarakis, G. Xyloyris, X. Masip-Bruin, J. Martrat	IEEE Access
Dynamic deployment and security assessment of resilient Services over Digital Twins	Juan Tamboleo, Alejandro Molina Zarca, Fabrizio Granelli, Jose Manuel Manjón, Antonio Pastor, Antonio Skarmeta and Diego Lopez	EuCNC 2024

2.1.6 Project videos

The HORSE project has a YouTube channel for its videos. So far 1 video has been published on the website, the Project Overview video.

The published video has generated 272 views. Figure 11 shows the social media card that was used for the promotion of the video.

Figure 11: HORSE Overview video promotional card

2.1.7 Digital and printed promotional materials

The HORSE project started in the post COVID world which meant that activities were mostly taking place requiring physical presence. HORSE participated in the ETSI Conference 2023, where a project overview poster was presented. During this time a 4 page flyer was created, on A4 size. This flyer was taken in different events, eg. Mobilie World Congress 2023, EuCNC 2023, ETSI conference 2023. Another version of flyers was created in postcard size for the ease of carrying and distributing.

All promotional materials are printed as well as uploaded on the website.

Figure 12: HORSE Postcard flyer (front and back)

Figure 13: HORSE Overview flyer

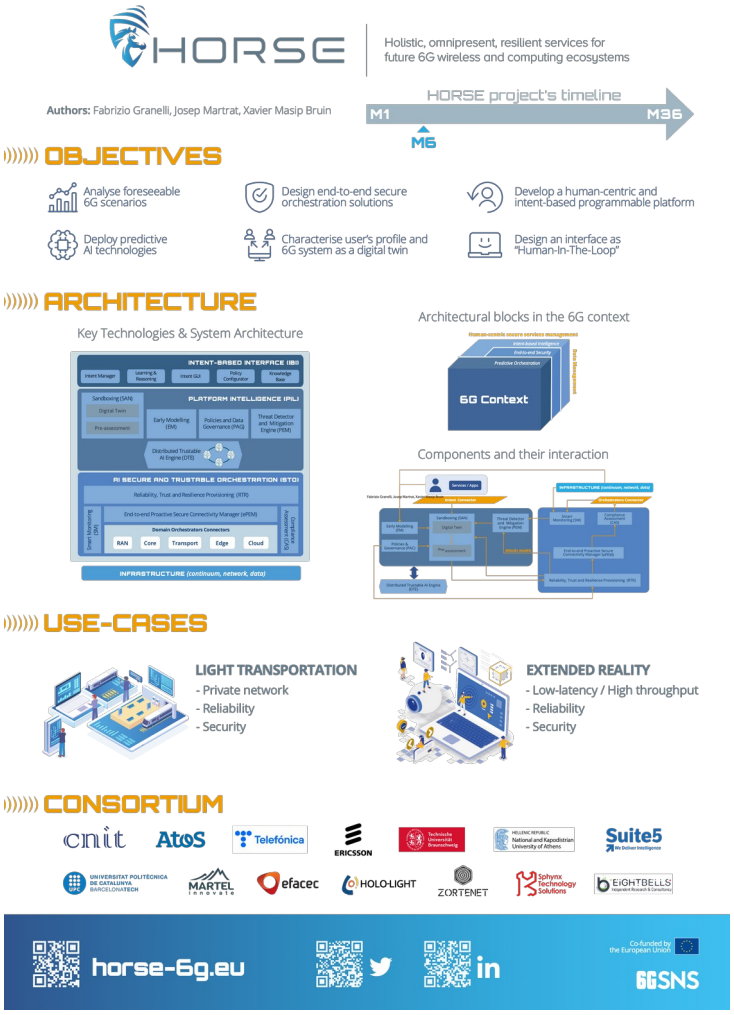


Figure 14: HORSE Overview poster

2.1.8 Events

Event organization and attendance are an important aspect of the HORSE communication and dissemination's strategy. Since the project kicked off in January 2023, HORSE coordinator and project partners have taken a very proactive step in raising awareness about the project in the European and global 6G community.

Table 2 provides further details on attended events for the reporting period.

Table 2: HORSE Events overview

Name of the event	Date, Location	Event website	Type of contribution	Partners involved
ETSI Research conference	Nice, 6-9 Feb 2023	https://www.etsi.org/events/2130-etsi-research-conference	Presentation, poster presentation	CNIT, Martel
6G SNS Webinar series	Online, 23 Feb 2023	https://smart-networks.europa.eu/event/sns-lunchtime-webinar-3-introducing-the-sns-projects-part-3-of-4/	Presentation	CNIT, Martel
Mobile World Congress 2023	Barcelona, 27 Feb-2 Mar 2023	https://www.mwcbarcelona.com/	Participation	Martel
EuCNC 2023	Gothenburg, Sweden, 6-9 June 2023	https://www.eucnc.eu/2023/www.eucnc.eu/index.html	Poster presentation	CNIT, Martel, Telefonica
GlobeCom 2023	Kuala Lumpur, 4-8 Dec 2023	https://globecom2023.ieee-globecom.org/workshop/ws13-path-towards-6g-standardization-and-research-vision	Paper presentation	CNIT
Symposium on vision and facts on 6G and future networks in Europe	Baltimore, USA, 15 Nov 2023	https://fnwf2023.ieee.org/program/symposiums/symposium-vision-and-facts-6g-and-future-networks-europe	Symposium chair, paper presentation	University of Murcia
10th annual Control Systems Cybersecurity Europe and UK	London, 7-8 Nov 2023	https://www.cybersenate.com/control-system-cybersec-europe-uk/		
Hexa-X webinar	Online, Jan 26th 2024	https://smart-networks.europa.eu/event/hexa-x-ii-workshop-on-26-january-online-event/	Presentation	CNIT

Hexa-X webinar	Online, Feb 14th 2024	https://smart-networks.europa.eu/event/the-6g-series-workshop-by-hexa-x-ii/	Presentation	Atos
Mobile World Congress 2024	Barcelona, 26-29 Feb 2024	https://www.mwcbarcelona.com/	Participation	HOLO Light, Martel
24th IEEE/ACM international Symposium on Cluster, Cloud and Internet Computing	May 6-9, 2024 Philadelphia, USA	https://2024.ccgrid-conference.org/	Paper presentation	UPC, NKUA, TUBS, TID
EuCNC 2024	3-6 June 2024, Antwerp	https://www.eucnc.eu/	Presentation	Telefonica, HOLO Light, Martel
DSP Leaders World Forum 2024	5-6 June 2024, Windsor	https://www.telecomtv.com/content/dsp-leaders-forum-agenda-day-2/	Panel	Telefonica

Planned events

HORSE is planning to host 2 workshops at the upcoming IEEE CAMAD 2024 conference (IEEE International Workshop on Computer Aided Modeling and Design of Communication Links and Networks), taking place from 21st-23rd October 2024 in Athens, Greece.

- **Workshop: Security and Digital Twins in 6G:** The advent of 6G technology promises to revolutionize the digital landscape by providing unprecedented speed, reliability, and connectivity.
  However, with great power comes great responsibility, and the security of these networks is paramount and should be studied in depth to achieve a 6G “secure by design”. On the other hand, digital twins, as virtual replicas of physical systems, play a crucial role in simulating and analyzing 6G environments. This special issue seeks to explore the integration and intersection of security and digital twins within the context of 6G technology.
- **Workshop: Addressing 6G Cybersecurity and Privacy Challenges:** Cybersecurity and Privacy are of utmost importance in beyond-5G and future 6G network. 6G concepts will continue evolving towards release 21+ 3GPP, also leveraging developments from European SNS JU initiative. To address cybersecurity challenges in advance is paramount while system is designed. Key trends of the 6G landscape, in addition to their obvious technical and business value, as expected, are accompanied with a drastic increase in the attack surface compared to legacy cellular network infrastructures.

The call for papers for the first workshop «Security and Digital Twins in 6G» has been shared with the entire 6G SNS community, inviting scientific papers from different projects and/or research and academic organisations.

The second workshop, «Addressing 6G Cybersecurity and Privacy challenges», is an invitation based workshop, with a collaboration between projects HORSE, PRIVATEER and RIGOUROUS. Flagship project HEXA-X II is also invited for its contribution on the architectural aspects and their impact on 6G security. In the second half of the workshop, the new SNS Stream B-01-04 projects will be invited to present their key research topic.

3 Collaboration and liaisons with other projects and initiatives

3.1 Liaisons within the SNS-JU landscape

In Task 6.2, HORSE's goals is to create synergies with other initiatives. To this end, we reached out to other SNS projects in the Stream B, and the European 5G/6G community, informing them about HORSE's aims and objectives and inviting them to share information on their project with us. Below is a list of the projects approached for collaboration. The objective for creating these connections is to facilitate a cross dissemination of both actions via shared-blog entries, cross-referral on the project websites, mutual social network interaction and event sharing perspective and to have a constant flow of communication between the initiatives in order to promote additional points for collaboration which may emerge in the short and mid-term. Martel, leading the communication dissemination and community building task participates in the monthly SNS JU communication task force calls where updates from the project are shared as well as information about events, CFPs, news items, blogposts etc.

HORSE is organising a full day workshop at the upcoming CAMAD 2024 conference in the field of cybersecurity and privacy for 6G communication networks, in collaboration with PRIVATEER and ROGOUROUS projects, of the SNS Stream B. Please see section 2.1.8 for more details.

HORSE project is invited (partner Telefonica) to take part in the discussions on the contents of a whitepaper the 6G-IA is preparing on its vision for next-generation networks. The whitepaper focusses on the activities planned or performed by the flagship project Hexa-X-II. For the HORSE project this is interesting and advantageous what is an advantage for us, as we have managed to include our NDT approach into the enablers Hexa-X-II is considering for security and privacy. Furthermore, given there is a section on NDT (just one page, given the nature of the paper) I have included my name to provide a contribution on this, on behalf of HORSE.

4 Impact assessment

4.1 Communication and dissemination KPIs

The following metrics, Table 3, are used to monitor and assess the progress of the communication and dissemination activities and provide some measurable outcomes related to their impact created (as far as this is feasible from a quantitative point of view).

Table 3: HORSE's communication KPIs

Tool/activity	KPI	Target value	Value at M18
Website	Unique visitors average (yearly)	>3000	3917
Social media	Number of followers (by project end) on Twitter Number of followers (by project end) on LinkedIn	500 150	251 361
White papers	Number of published white papers	3	1 in pipeline
News items on website	Number of published news items	≥ 20	12
e-Newsletters	Number of newsletters sent out	6	2
Flyers/ Brochures Presentations Posters/Roll-Ups	Number of flyers/brochures (incl. digital brochures) Number of project presentations Number of produced posters/roll-ups	3 6 3	2 2 2
Videos	Number of produced videos	6	1
Workshops	Number of attended/organized workshops	3	2 planned at CAMAD
Webinars, panels, demos	Webinars Panels Demos	3+ 3+ 3+	3 1 0
Trainings (online/in-person)	Number of courses offered	2	1
Scientific publications	Number of publications	15+	8
Participation in events & presentations	Number of external events partners attended to promote the project, events per including scientific conferences, and	5 per year	14

Tool/activity	KPI	Target value	Value at M18
	year industrial technology venues		
Standardization contributions	Number of contributions to standardization fora	6	50 contributions (explained in section 12)
Open-source contributions	Number of contributions to open-source initiatives	3	--
Policy strategies contributions	Number of policies contributed with recommendations	>3	--

4.2 Impact Creation Deliverables and Milestones

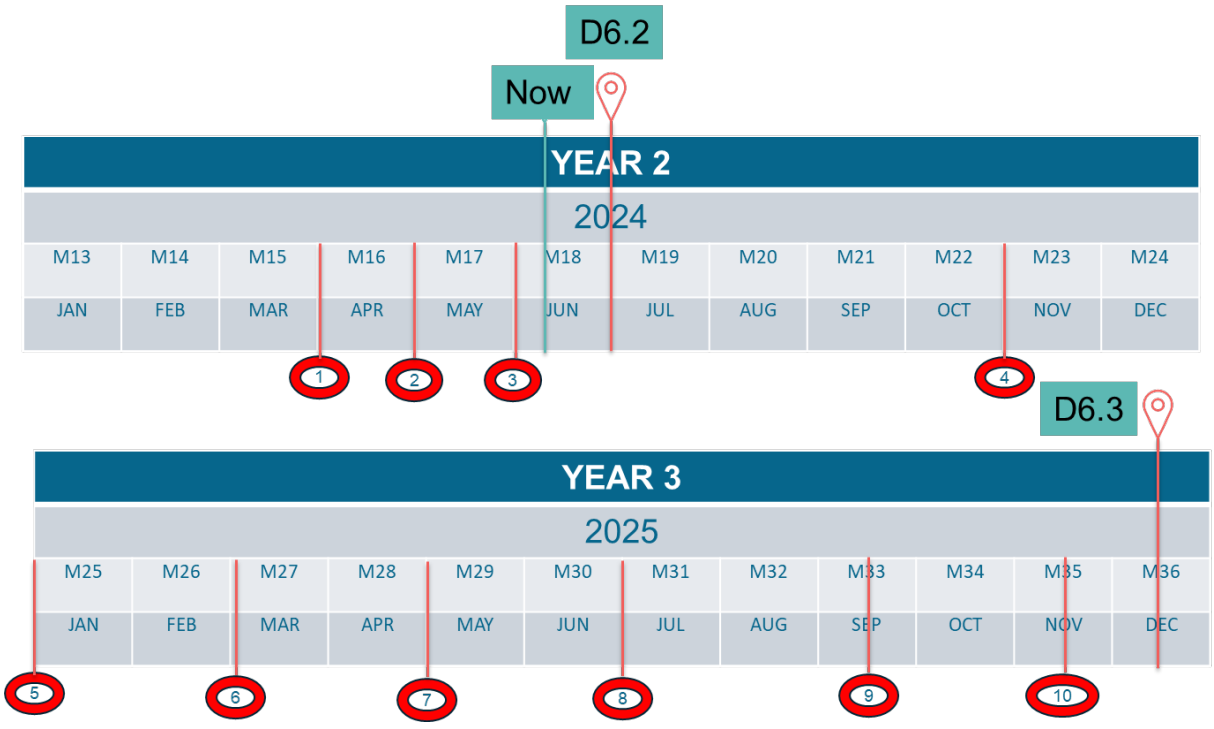
Table 4: HORSE impact creation deliverables and milestones

Number	Name	Lead partner	Dissemination level	Due Date	Status at M18
D6.1	**Impact Creation Strategy and Plan**	MARTEL	PU	M05	Submitted
D6.2	**Impact creation report and exploitation strategy**	MARTEL	PU	M18	Current document
D6.3	**Final impact creation report and exploitation plan**	8BELLS	PU	M36	Expected delivery in M36

5 Exploitation Activities and IPR Management

5.1 General Strategy

In the first 18 months, HORSE developed a comprehensive roadmap outlining key milestones, tools, methods and overall work on the exploitation aspects of the project. We conducted detailed SWOT and PESTLE analyses, and described a Lean Canvas model to establish a solid approach on the integration of HORSE in the market. Focus was also given on identifying and managing intellectual property rights (IPR) of the assets developed in this iteration, compiling an overview of HORSE's results, and creating an exploitation and valorization plan. This included the identification of Background (BG) and Foreground (FG) intellectual property (IP), exploitable results (ER) as well as the project's key exploitable results (KER) with a respective exploitation pathway for each result. ERs refer to any output generated during the project's implementation that has potential value for further use and commercialization while KERs are the most critical and high-impact results among the ERs. Each partner also elaborated on their exploitation plan, i.e. how they individually plan to benefit from their participation in HORSE. Additionally, a preliminary market analysis was conducted for the cybersecurity and 5G security markets, focusing on market ecosystems, trends, revenue forecasts, and dynamics. The initial phase also involved aligning the project's goals with the United Nations Sustainable Development Goals (UNSDG), particularly in resilient infrastructure and sustainable communities.



In the next 18 months (IT-2), the project will enhance and update the initial analyses and strategies based on new insights and feedback. The roadmap will be continuously updated to reflect achieved milestones and strategic shifts. Advanced SWOT and complete Lean Canvas models will be developed, and a full PESTLE analysis will be conducted, integrating these results into strategic planning. The IPR Matrix Methodology will be refined to adapt to new ERs and feedback, and individual exploitation plans will be enhanced through deeper collaboration with partners. Market analyses will be regularly updated to include emerging

technologies and competitors, while new strengths, weaknesses, opportunities, and threats will be identified. The project will intensify its focus on contributions to the European Union (EU), tracking progress and ensuring alignment with the UN 2030 Agenda, particularly in the areas of resilient infrastructure, innovation, and sustainable communities.

The milestones (MS) shown above, include both past and future milestones. The past milestones include the list of goals we have set in order to gather the results presented in D6.2, these are:

- MS1: Collect FG and BG IPs, ER by each partner and identify HORSE's KERs.
- MS2: Conduct Market Analysis in order to demonstrate that HORSE fits in the cybersecurity market.
- MS3: Integrate the results we gathered in D6.2.

The future milestones are a set of goals HORSE's consortium has set in order to complete the exploitation activities of HORSE and reach D6.3. These milestones are:

- MS4: The consortium will review, if the Horizon Results Booster [25] services will be used and initiate any procedures accordingly. Duration: 6 months.
- MS5: Update FG, BG IPs, ERs and KERs. Duration: 2 months.
- MS6: Conduct HORSE's business analysis. Elaborate on the use cases and fill in the lean canvas we demonstrate in Chapter 2. Duration: 2 months.
- MS7: Develop Joint Exploitation Plans. Duration 2 months.
- MS8: Final deadline, to gather any missing results.
- MS9: Present 1st ToC of D6.3.
- MS10: 1st draft of D6.3.

5.2 Methodological approach

In this section, the methodological approach along with the tools that are employed to perform the Market and Business analysis are presented. More specifically, for the Market analysis, cybersecurity, 5G security and the AI ecosystems are explored, and the market trends are thoroughly illustrated. Additionally, a preliminary SWOT analysis is performed that enables the identification of internal and external factors that might affect the market position of the HORSE system. In addition to the Market analysis, a business analysis also takes place. To strategically unfold the business model of the Horse project, a lean canvas for each ER has been developed. Finally, conducting a PESTLE analysis empowers the consortium to navigate the dynamic business landscape effectively, capitalize on opportunities, and mitigate potential challenges, thereby enhancing the system's competitiveness and resilience.

5.2.1 SWOT Analysis

A SWOT analysis is a strategic planning tool that helps companies assess their internal strengths and weaknesses, as well as external opportunities and threats [1]. It provides a systematic framework for determining the present condition of an organization or a specific project. Here is a description of SWOT analysis and its theoretical framework:

- **Strengths:** Strengths are internal features, resources, and talents that give a firm or project a competitive advantage. These could include a talented workforce, a strong brand, efficient operations, or proprietary technology.
- **Weaknesses:** Weaknesses are internal flaws that impair an organization's or project's performance. These might involve areas where the business lacks resources, skills, or efficiency, thus putting it at a competitive disadvantage.
- **Opportunities:** Opportunities are external factors or conditions in the environment that have an opportunity to benefit a business or activity. These could include emerging markets, altering consumer preferences, technological breakthroughs, or political developments.
- **Threats:** Threats are external variables or conditions that may have a negative impact on an organization or project. Competitiveness, economic downturns, legal issues, and changing market trends are all possible threats.
- **Analysis:** Companies use the identified strengths, weaknesses, opportunities, and threats to get insight into their strategic positioning. This analysis helps with decision making, goal setting, and plan development.
- **Action Planning:** SWOT analysis is used by organizations to develop action plans to use their strengths, address weaknesses, capitalize on opportunities, and mitigate threats. These plans guide the organization toward its aims.

SWOT analysis draws from several theoretical concepts and principles:

- Strategic Management: SWOT analysis is an important tool in strategic management, a field that focuses on designing and implementing strategies to meet company goals.
- Resource-Based View (RBV): The concept of strengths and weaknesses in SWOT is linked to RBV theory, which highlights that an organization's unique resources and capabilities are sources of competitive advantage.
- Environmental Scanning: The recognition of opportunities and threats in SWOT analysis highlights the importance of environmental scanning, a strategic management method that involves monitoring and evaluating external factors that influence an organization.
- SWOT Matrix: A SWOT matrix is a commonly used tool for visualizing SWOT analysis results, classifying internal aspects as strengths and weaknesses and external factors as opportunities and threats. This matrix is a simplified representation of the strategic issues that a business faces.
- Strategy Formulation: SWOT analysis is closely tied to strategy formulation since it helps organizations identify potential paths and prioritize efforts to achieve their objectives. This technique is in line with strategic planning and decision-making theories.
- Competitive Analysis: SWOT analysis is commonly used in competitive research to help organizations assess their position relative to competitors and identify areas where they can gain a competitive advantage.
- Strategic Planning Models: SWOT analysis can be included into a variety of business planning frameworks, such as the standard strategic planning process, the Balanced Scorecard, and the McKinsey 7S framework, to provide a comprehensive assessment of an organization's strategy.

In summary, SWOT analysis is a useful tool based on strategic management philosophy. It offers an organized method to assess the internal and external factors that impact a

company's success, enabling more informed decision-making and the development of effective initiatives.

5.2.2 Lean Canvas

The Lean Canvas is a one-page business model template designed to help entrepreneurs and startups quickly visualize and validate their business ideas. It was developed by Ash Maurya [2] based on the Lean Startup methodology pioneered by Eric Ries.

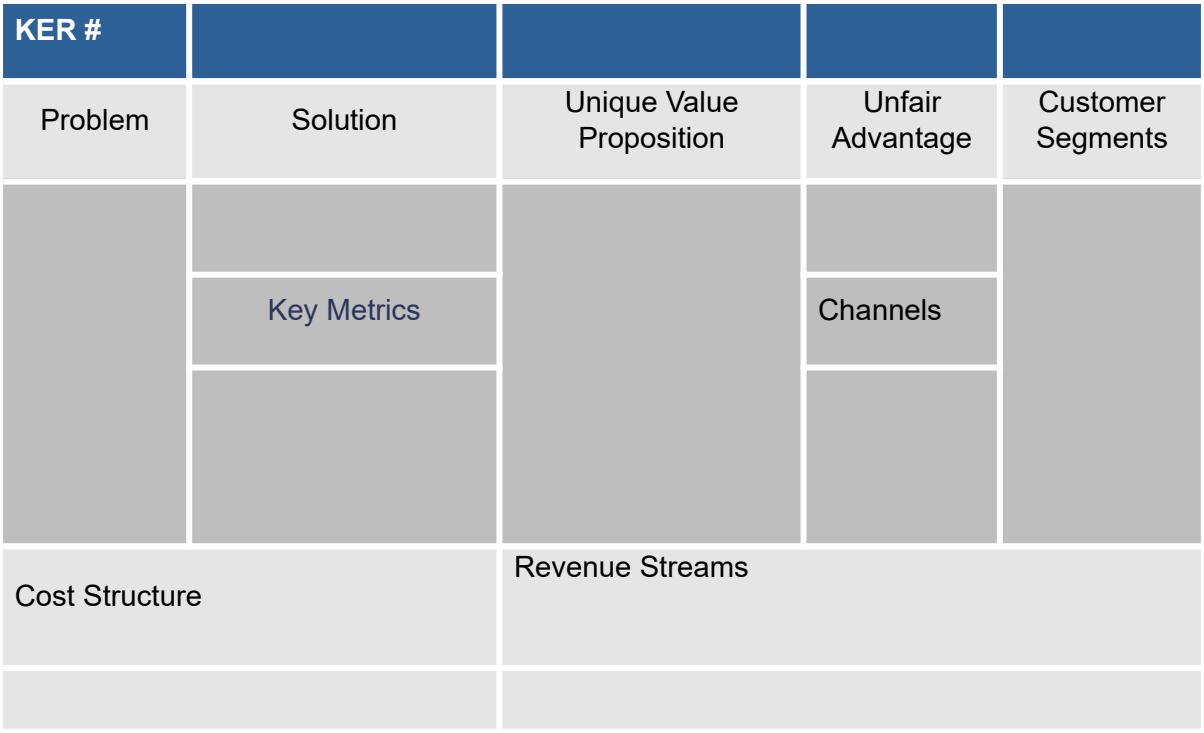


Figure 15: Lean Canvas Example

The Lean Canvas as shown in Figure 15, consists of nine key building blocks:

- Problem: The top one to three issues that your target clients are having are listed in this block. It's critical to specify the wants or pain areas that the product or service seeks to solve.
- Solution: Here, a description of the special solution for the issues that have been found is provided. This could be a platform, service, or product that addresses the problems more successfully or economically than the options now available.
- Key Metrics: Choose the most crucial KPIs that will show whether the product or service is succeeding. These KPIs might be conversion rates, customer lifetime value, acquisition costs, etc.
- Unique Value Proposition: This section explains how the solution differs from and outperforms the current options. It should make clear to consumers the special advantages that the good or service provides.
- Unfair Advantage: Determine if the product or service has any special benefits or entrance obstacles. This could include unique alliances, specialized knowledge, intellectual property, or other elements that provide venture with a competitive advantage.

- Channels: Channels describe how a corporation communicates and interacts with its customers. It includes sales channels, distribution routes, marketing channels, and communication strategies.
- Revenue Streams: This block describes how the company makes revenue from its client segments. It covers price strategies and revenue streams.
- Cost Structure: Cost Structure refers to all of the expenses associated with running a firm. It includes fixed and variable costs.

5.2.3 PESTLE Analysis

Businesses may assess and understand the external macro-environmental elements that can affect their operations by using a PESTLE study, which is a strategic tool. Political, Economic, Social, Technological, Legal, and Environmental issues are all included in the acronym. A category of effects that can have an impact on the business environment is represented by each of these components [3].

- **Political Factors:** These refer to how the corporate environment is impacted by laws, rules, political stability, and trade agreements. Trade restrictions, government stability, taxation policies, and political ideologies are examples of political influences.
- **Economic Factors:** Economic factors include general economic conditions, such inflation, interest rates, growth in the economy, and unemployment rates, that can influence enterprises. To understand consumer purchasing trends, market developments, and general economic stability, businesses evaluate economic fundamentals.
- **Social Factors:** Social factors include factors like demographics, cultural conventions, and changes in lifestyle that have an impact on consumer preferences and behavior. Businesses modify their goods and services to match changing customer demands by taking into account variables like social attitudes, lifestyle trends, demography, and cultural values.
- **Technological Factors:** Technological variables encompass innovations, automation, digitization, and technological breakthroughs which have the potential to change sectors and generate new business opportunities. To stay competitive and take advantage of evolving technologies, businesses evaluate infrastructure advancements, digital transformation, research and development efforts, and technical trends.
- **Legal Factors:** Laws, rules, and legal frameworks that control corporate operations and industry standards are examples of legal factors. To maintain legal compliance and reduce risks, businesses examine legal aspects related to labor laws, consumer protection laws, industry-specific legislation, intellectual property rights, and compliance requirements.
- **Environmental Factors:** Environmental variables include ecological aspects which can affect business operations and sustainability, natural disasters, climate change, and environmental sustainability. To reduce their environmental impact and profit from green initiatives, businesses assess environmental variables like carbon footprint, resource scarcity, environmental restrictions, and sustainable practices.

6 Exploitation, IPR in the first period of the project (IT1)

6.1 IPR Matrix Methodology

The HORSE IPR management approach, as mentioned above, foresees the utilization of an IPR Matrix in order to define the main IPR issues concerning the HORSE Innovation and IPR Management Strategy. This approach will support all project partners in identifying and managing the BG, FG knowledge, and ERs of the project, in order to have a full overview of any IP protection measures and necessary agreements that will enable a successful exploitation of the project's offerings.

The IPR Matrix methodology is comprised of 4 distinct but interconnected steps, as follows:

- **Step 1:** Identification of the BG IP and definition of access rights among partners within the project.
- **Step 2:** Identification of all assets and results, which constitute the FG IP of the project and are foreseen to be generated under the HORSE activities.
- **Step 3:** Identification of the project's ERs (as defined at this stage of the project) and the corresponding type of interest for their further exploitation, including commercialization, along with the contributing partners to each result.
- **Step4:** Update the project's initial KERs and the corresponding type of interest for their further exploitation, including commercialization, along with the contributing partners to each result.
- **Step 5:** Update the project's key innovations based on the current state of the project.
- **Step 6:** Definition of a preliminary framework of IPR protection measures and exploitation pathways per partner for the defined HORSE results, which will enhance their further exploitation and commercialization.

At this stage of the project, the objective of the Innovation and IPR Management Strategy of HORSE is to define the main results and identify, to the extent possible, the BG and FG IPs of the project along with their corresponding access rights. During the later stages of the project's implementation, the IPR methodology will be updated accordingly, in order to capture and integrate the evolvement of the identified results and IPR approach as the project results become further specified and available. In particular, the identification of ERs would yield the need to establish an ownership regime among project partners and to define the most suitable exploitation pathways for each one of the ERs. In addition, rules and conditions to get access to ERs need also to be considered, as well as the main target groups of external stakeholders and the potential benefits and added value they stand to gain from the HORSE ERs. Finally, validation of the IPR needs to be meticulously employed.

Table 5: HORSE IPR Matrix

Background (BG)	Foreground (FG)	Exploitable Results (ER)	Key Exploitable Results	Innovations

			(KERs)	
• BG # • Relevant Background • Background Number • Short Description • TRL • Type of Protection • Type of utilization within HORSE • Conditions to use outside of HORSE • Interest in further exploitation through HORSE results	• Work Package • Project Results (PR) • Main Contributing Partner • Further Contributing Partner(s) • Foreground Number • Short Description of FG • TRL • Type Of Protection • Conditions to Use within HORSE • Interest in further commercialization of project results • Conditions to use after the end of the project	• Er Number • Exploitable Result • Short Description • Main Partner(s) • Contributing Partner(s) • BG number (related) • FG number (related) • Proposition of ER – Owner (if any) • Relevance of IP protection (if any) • M-making them and selling them • U – Using them • L - License them • S - Providing them as a service • O - Others • Most Promising Path • Further Comments	• KER number • Key Exploitable Result • Short Description • Main Partner(s) • Contributing Partner(s) • FG Number (related) • BG Number (related) • Licensing • Proposition of ER – Owner (if any) • Relevance of IP protection (if any) • M-making them and selling them • U – Using them • L - License them • S - Providing them as a service • O - Others • Most Promising Path • Further Comments	• Innovation ID • Key Innovation to Research • Lead Partner • TRL • Rationale (Means Of Verification)

6.1.1 Identification of Background

In the first part of the IPR Matrix, the BG that will be used during the project's implementation shall be identified, as illustrated in Table 6.

Table 6: HORSE IPR Matrix - BG IP

#	Relevant Background	Contributing Partners	Background Number	Short Description	TRL	Type of Protection	How it will be utilized within HORSE	Conditions to use within HORSE	Conditions to use outside HORSE	Interest in further exploitation through HORSE results

In the second column of this part of the IPR Matrix, the project BG results to be deployed at this stage of the project are listed. In the third column, the name of the partner who owns this BG is indicated. For each identified BG required for the creation of the result, a specific BG number per partner has been assigned. In column 4, the corresponding WP number of the project within which the BG falls is indicated, while column 5 includes a short description of the BG. In column 6 partners indicate the TRL o their asset in MO1 and the level of the TRL they expect to reach by the end of the project (M036). In column 7, partners indicate relevant IP protection types for the BG in terms of patents, copyright, etc., while additional information regarding the utilization of the BG within HORSE can be found in column 8. In the 9th column, the conditions to use the BG within the project (e.g., free to use or subject to charges, etc.) are indicated by each partner, whether there are any restrictions to use the BG or not. In the 10th column, the BG's condition to use outside HORSE is indicated, while in the last column partners shall mention if they have any interest in exploitation/commercialization of the relevant BG through the project results.

6.1.2 Identification of Foreground IP

In the second part of the IPR Matrix, the FG of the project is registered, as presented in Table 7.

Table 7: HORSE IPR Matrix - FG IP

Work Package	Project Results (PR)	Main Contributing Partner	Further Contributing Partner(s)	Foreground Number	Short Description Of FG	TRL	Type of Protection	Conditions to use within HORSE	Interest In Further Commercialization of Project Results	Conditions to use after the end of the project

In the first column, the Work Package (WP) number associated with each HORSE result is listed. The second column details the specific project result. The third column indicates the main contributing partner responsible for that result, while the fourth column lists any further contributing partners. Each result is assigned a unique FG number in the fifth column. The

sixth column contains a short description of the FG. The Technology Readiness Level (TRL) is noted in the seventh column, both the initial TRL of the IP and the expected TRL at the end of the project need to be listed. The eighth column specifies the type of protection, such as patents or copyright. In the nineth column, the conditions for using the FG within HORSE (e.g., free to use or subject to charges) and any usage restrictions are indicated. The tenth column allows partners to express their interest in the further exploitation of the project results. Finally, the eleventh column details the conditions for using the FG after the project's conclusion, such as whether it is free to use or subject to a license fee.

6.1.3 Identification of Exploitable Results and Key Exploitable Results

Based on the identified FG, the HORSE consortium delineated the ERs along with the associated IPR management procedures, such as protection measures, the definition of access rights, and exploitation pathways. Additionally, the consortium updated the initial KERs of the project to ensure they reflect the latest developments and potential impacts.

During this phase, the third part of the IPR Matrix was developed to detail the ERs and identify the primary contributors to these results. The fourth part of the matrix is dedicated to the KERS, where we also try to identify primary contributors, exploitation paths etc. The main objectives of these part of the IPR Matrix are:

- To ascertain IP ownership and exploitation claims, and proactively identify potential conflicts for each ER and KER.
- To facilitate informed decisions regarding the IP protection of an ER, ensuring timely progression through the necessary steps, which may include potential IP agreements (e.g., joint ownership agreements, access rights provisions, or NDAs for confidentiality).

In this context, Table 8 and Table 9 provide a visual representation of the aforementioned segment of the IPR Matrix.

Table 8: IPR Matrix - Exploitable Results

ER Number	Exploitable Result	Main Contributing Partner	Further Contributing Partners	FG number (related)	BG number (related)	Proposition of ER – Owner (if any)	Relevance of IP protection (if any)	M-making them and selling them	U – Using them	L - License them	S - Providing them as a service	O - Others	Most Promising Path	Further Comments

In the first column, the ER number is listed, providing a unique identifier for each ER. The second column contains the name of the ER being listed. The third column includes a brief description of each ER. The fourth and fifth columns describe the main contributing partner and the further contributing partners, respectively. The sixth column associates the ER with a listed FG IP asset related to this ER, while the seventh column associates the ER with a listed BG IP asset. The eighth column provides information on the licensing status of the KER. Additionally, the nineth column provides information on the licensing of each individual ER, such as Open Source, Apache 2.0, etc., while the tenth column highlights the relevance

of IP protection for the KER. The specifications requested in these columns can sometimes be omitted due to the maturity of the project and the determination of the partners to claim ownership of a KER. The last six columns are used to determine a clear and comprehensive exploitation path for each partner listing an ER and will be analyzed in section 6.1.4.

Table 9: Key Exploitable Results

ER Number	Exploitable Result	Main Contributing Partner	Further Contributing Partners	FG number (related)	BG number (related)	Licensing	Proposition of ER – Owner (if any)	Relevance of IP protection (if any)	M-making them and selling them	U – Using them	L - License them	S - Providing them as a service	O - Others	Most Promising Path	Further Comments

6.1.4 Identification of Exploitation Pathway per Result

Even when partners share a common interest in exploitation, their strategies for the optimal exploitation pathway to maximize the impact of each ER can vary due to strategic differences and priorities. Defining the exploitation pathway is as crucial as determining the optimal measures for IP protection. Therefore, it is imperative to outline the desired exploitation pathways among HORSE partners.

Table 10: HORSE IPR Matrix - Exploitation Pathway/Partner/Result

ER number	Main Partner(s)	M-Making them and selling them	U - Using them	L - License them	S - Providing as a Service	O - Others	Most promising path

As shown in Table 10, the second column lists the partners involved in the project, while the first column indicates the corresponding number for each ER, as defined in Table 8. The exploitation pathways table is included in Tables 8 and 9, where partners have filled each cell with one or more letters to indicate their desired exploitation pathways, as follows:

- M: Making a product and selling it.
- U: Using the project result internally for further development, for instance:
  - To develop something else for sale.
  - For R&D departments (public/private) to use results in new research projects.
- L: Licensing the project result to third parties.
- S: Providing a service, such as consultancy, etc.
- O: Others.

- Most Promising Path: The most probable course of action from all of the above. For example, it is almost certain that before selling a product an organization should license it, making Licensing a very promising exploitation path.

The contributing partner for each ER should select the appropriate exploitation claims in consultation with the contributing partners, the Project Coordinator, and the IPR and Innovation Manager. This process creates a matrix that demonstrates the desired exploitation pathways of each contributing partner for every result to which they have contributed, along with insights into the most prominent exploitation pathways for each result.

6.1.5 Updated HORSE Innovations

The HORSE project has identified various preliminary Innovations that are listed inside the original Grand Agreement. They are also listed in the fifth segment of the IPR matrix in order to be updated based on the project's current status.

Table 11: HORSE IPR Matrix - Innovation

Innovation ID	Key Innovation to research	Lead Partner	TRL	Rationale (Means of Verification)

The table includes several key columns. Innovation ID is a unique identifier assigned to each innovation for easy tracking and reference within the project. The second column provides the key Innovation to research and showcases a brief description of the main innovation being investigated or developed. Columns number three includes the lead partners, i.e. the organization or entity responsible for leading the research and development of the key innovation. As in previous examples column number four denotes the TRL of the innovation, indicating its stage of development, from initial concept (TRL 1) to full deployment (TRL 9). Finally, "Rationale or Means of Verification" outlines the justification for the innovation, including the methods and criteria used to verify its progress and success.

6.2 Overview Of HORSE's Results, Background and Foreground IP

6.2.1 Identified Exploitable Results of HORSE

The main results of HORSE, as identified and updated by the consortium at the interim stage of the project, along with their description and the corresponding ER number, are presented in Table 12.

Table 12: HORSE Identified Exploitable Results

ER number	Exploitable Result (ER)	Short Description
ER1	**RTR**	Generation of Ansible playbooks via a mitigation action, in order to defend against threats.
ER2	**PEM**	Predictive threat detector and mitigation driver for the analysis

		and processing of network streams in complex network and infrastructure scenarios.
ER3	**SAN & NDTs**	Sandbox and Network Digital Twins used for prediction, prevention and what-if analysis
ER4	**EM**	Framework for the modeling of vulnerabilities, threats, attacks, proactive actions, mitigations, and estimated impacts.
ER5	**IBI**	A collection of tools that proposes low-level network policies in response to security threats and vulnerabilities detected in the network based in high-level user's intents related to resiliency, quality of service, and availability.
ER6	**PAG**	Experiment on and implement new encryption, anonymization and data observability techniques. Upgrade of Suite5 services portfolio of data-driven intelligence with 5G/6G specific technological and innovation know-how.
ER7	**Pre-Processing**	8BELLS presents a middleware solution designed to orchestrate and bolster a wide array of data sources, ranging in scale and structure, within cohesive and scalable data environments.

6.2.2 Identified Key Exploitable Results of HORSE

The main KERs of HORSE, as identified and updated by the consortium at the interim stage of the project, along with their description and the corresponding ER number, are presented in Table 13.

Table 13: HORSE Identified Key Exploitable Results

ER number	Exploitable Result (ER)	Short Description
KER1	**HORSE platform**	Complete set of features and functionalities towards a secure 6G system orchestration.
KER2	**Distributed AI Engine for Services Preassessment**	Set of functionalities (Sandboxing, AI contextual models, etc.) to be used to replicate the entire 6G landscape in order to conduct a preliminary performance assessment of the tentative orchestration strategies to be deployed, aimed at ensuring that all deployed services run in a secure, distributed and optimized environment.
KER3	**Smart Monitoring (SM)**	Responsible for the collection of data from all various and diverse domain resources, as well as data related to the usage of the resources involved in the lifecycle management.
KER4	**Threat Detector and Mitigation Engine**	Tool responsible for detecting threats in a predictive form, thus proactively acting towards removing or in the worst case mitigating the impact of the foreseen threat.

KER5	**Intent-based Secure cross-Domain Orchestrator**	Includes a set of tools to logically and physically interact with the infrastructure elements to provide a secure cross-domain orchestration. The interaction will be handled through a proper mapping of high-level intents into security workflows able to react to security threats and vulnerabilities.
KER6	**Secure e2e connectivity Manager**	In charge of service orchestration, which supports recursive deployment of many functional components for multi-tenancy, high device heterogeneity through virtualization, end-to-end resource self-configuration, and most importantly the provision of a secure framework that can span across multiple domains and applications.
KER7	**Network Digital Twin**	An environment for testing "what-if" scenarios and performing predictions on the state of the network. The Network Digital Twin represents an isolated environment which accurately replicates the original 6G network as well as services and traffic.

6.2.3 Background IP

In the interim version, the project partners were able to examine in retrospect and update the BG IP to be used so as to achieve the objectives of HORSE. This is presented in Table 14.

Table 14: HORSE Identified IP BG

#	Relevant Background	Contributing Partner (Partner Name)	Background Number (First number refers to WP relevance, second number refers to assets order)	Short Description of BG	TRL M01 -> TRL M036	Type of Protection (patent, coyright, TM, Utility model , Open source…)	How will it be utilised within Project?	Conditions to Use within the Project (free to use, licence fee, restrictions, NDA..)	Conditions to use outside the Project *E.g. Is it confidential? Can it be shared with externals? Is it currently shared with externals? If yes, on what conditions?*	Interest in further exploitation through Project results (Yes/No)
1	DFF	8BELLS	BG4.1	The Data Format Fusion (DFF) aims to bring data-level interoperability and analytics between heterogeneous IoT devices and other functional data pipelines. It is designed based on open source standards and tools.	3 -> 5	Copyright	As a data distribution platform	free to use within the project	Subject of licensing agreement	yes
2	Comnetsemu network emulator	CNIT	BG4.2	Network Emulation environment, designed to emulate SDN, NFV and 5G networks.	2 -> 4	Opensource	As environment for the SAN	free to use within the project	Free to use	yes
3	Intent-based Resilience Orchestrator (IRO)	TUBS	BG5.1	A developed Intent-based resilience orchestration tool which uses Reinforcement Learning for Quality of Service assurance	6 -> 6	Opensource	As know-how and as framework for the IBI module	free to use within the project	Free to use	yes

6.2.4 Foreground IP

Considering the HORSE's results, the project partners were given the opportunity to update the FG IP, based on the overall progress of the project that occurred during the first half of implementation phase. The updated content in Table 15.

Table 15: HORSE Identified IP FG

WP	Project Result (PR) /Achievement	Main Contributing Partner (Partner Name)	Further Contributing Partner(s)	Foreground Number (First number refers to WP relevance, second number refers to assets order)	Short Description of FG	TRL M01 -> TRL M036	Type of Protection (patent, copyright, TM, Utility model …)	Conditions to Use within The Project (free to use, licence fee, restrictions, NDA..)	Interest in Further Commercialisation of Project Results (Yes/No)	Conditions to Use after the end of the Project (free to use, licence fee, restrictions, NDA..)
WP3	PEM	ETI	NKUA, UPC, ZORTE, 8BELLS	FG3.1	Predictive threat detector and mitigation driver for the analysis and processing of network streams in complex network and infrastructure scenarios.	2 -> 4	Other	Free to use	yes	Licence fee based on partners agreement
	NDT	CNIT/TID		FG3.2	Network Digital Twin environment for prediction, prevention and what-if analysis	2 -> 4	Other	Free to use		Free to use
	DTE	NKUA	ETI, TUBS,MAR	FG3.3	Distributed threat mitigation environment for the generation of either predictive or corrective intents	2->4	Other	Free to use	no	Licence fee based on partners agreement

	EM	UPC	ETI, NKUA, 8BELLS	FG3.4	Framework for the modeling of vulnerabilities, threats, attacks, proactive actions, mitigations, and estimated impacts.	2->4	Other	Free to use	no	Licence fee based on partners agreement
	PAG	SUITE5		FG3.5	A module which resolves and enforces access policies and data retention policies on the collected datasets (incl. a database which holds the access policies and the data retention policies - the collected datasets themselves are hosted on different HORSE platform component). The module also encrypts and anonymises the collected datasets, and logs the operations performed on the datasets of interest.	2->5	Copyright	Free to use within the project	yes	License fee based on multi-party exploitation agreements between Suite5 and the Party/ies involved in exploitation of results
WP4	ePEM	CNIT	ATOS, ETI, UPC, ZORTE, 8BELLS	FG4.1	ePEM plays a pivotal role in the HORSE security infrastructure. HORSE represents a cutting-edge security infrastructure designed to safeguard complex, distributed, and heterogeneous systems. In this intricate environment, the ePEM serves as a central architectural element, orchestrating ctions and providing observability over the various zomponents that constitute the end-to-end services secured within the HORSE security	2 -> 4	Other	Free to use	No	Free to use

					perimeter.					
	RTR	8Bells	8BELLS, EFACEC, UPC MAR, ATOS, CNIT ETI, ZORTE	FG4.2	Generation of Ansible playbooks via a mitigation action, in order to defend against threats.	2 -> 4	Copyright	Free to use	yes	Licence fee based on partners agreement
WP5	IBI	TUBS		FG5.1	The HORSE Intent-Based Interface is responsible for mapping high-level intents from a user, received as structured text or through a dedicated GUI, and further mapping those intents into use requirements. The requirements are then used to propose a list of deployable network policies that can mitigate attacks happening in the network or prevent future attacks. The policies are sent to a lower-level controller for deployment and enforcement in the network elements.	2 -> 4	Other	Free to use	no	Free to use

6.2.5 Innovations

Considering the HORSE's results, the project partners were given the opportunity to update the Innovations matrix, based on the overall progress of the project that occurred during the first half of implementation phase. The updated content in Table 16.

Table 16: HORSE Innovations

Innov ID	Key. Innov. To research	Lead Partner	TRL M01 -> TRL M036	Rationale (Means Of Verification)
I01	**Intent-based management interface**	TUBS	2 –> 5	An Intent management interface to automate the processing and deployment of the user intents and their interactions with other modules (D5.2, D5.3).
I02	**Attacks characterizatio n and modelling**	UPC	2 –> 4	Definition of a complete taxonomy of attacks models, to quantify the potential impact on the system (D3.1, D3.2).
I03	**Network Digital Twin environment**	TID / CNIT	2 –> 4	Availability of a network Digital Twin environment able to support the verification of end-to-end network scenarios, with specific focus on security (D3.1, D3.2).
I04	**Threat Detection and Mitigation**	ETI	2 –> 4	1 Innovation point: Among the different ML algorithms, a novel algorithm conceived in the Ericsson Labs and patent protected will be implemented and tested for the first time. Its performances will be compared with the current benchmarks. 2 The detector internal architecture is innovatively presenting a multi stage ML system where every stage learns from the outcomes of the previous one. This innovative scheme will allow many competitive benefits: a) A higher automation level (auto calculation of all the thresholds) b) A better visibility, that mean more effectiveness for combined or zero-day new forms of attacks. 3 At Horse framework level: The innovative combination of a Machine Learning threat detector And of a Digital Twin will innovatively allow a more effective mitigation strategy precisely dynamically modulating the required actions minimizing the network impairments.

I05	**End-to-end secure connectivity manager**	CNIT	2 –> 4	Availability of an end-to-end secure connectivity manager, an OSS module based on OSM, capable of orchestrating the requests by PIL to the available infrastructure domain (D4.1, D4.2).
I06	**Advanced placement for KNF**	MAR	2 -> 5	Ability to dynamically place cloud-native network functions based on intents and real time monitoring data within the ETSI OSM ecosystem (D4.1, D4.2).
I07	**Security for Advanced Communicatio n Techniques**	NKUA	2 –> 4	Investigation of PLS aspects related to the evolving 6G technologies, taking into account the energy efficiency and the signaling overhead (D3.1, D3.2).
I08	**Distributed Trustable AI Engine**	NKUA	2 –> 4	The target is to develop distributed AI solutions to secure the 6G network from unknown attacks (D3.1, D3.2).
I09	**Katana Slice Manager**	ZORTE	3 -> 5	Katana Slice Manager is a centralized software component that provides an interface for creating, modifying, monitoring, and deleting slices. Through the North Bound Interface (NBI), the Slice Manager receives the Network Slice Template (NEST) for creating network slices and provides the API for managing and monitoring them.
I10	**Security & Privacy Assurance Platform (STS)**	STS	4 -> 6	The security assurance platform combines runtime monitoring, dynamic and static testing, and impact assessments to provide a real-time security posture assessment and certification of heterogeneous systems (D4.1, D4.2).
I11	**Data Fusion Mechanism**	8BELLS	3->5	With regards to Smart Monitoring, 8BELLS offers a middleware solution in order to be able to orchestrate and support large scale and structurally different data sources under common and expandable data spaces. The above-mentioned mechanism greatly enhances data interoperability, through the adoption of common APIs for data exchange, and the definition of common data models. APIs for data and metadata management, as well as standardized endpoints for sophisticated queries are supported (D3.2, D4.2).

6.3 Exploitation and Valorization Plan

The current exploitation and valorization plan sets the stage of the Innovation and IPR Management Strategy, reflecting the overall progress and maturity of the HORSE project outcomes. Information for this plan was gathered from all HORSE partners, detailing recent project activities. The descriptions of the results (as identified in Sections 6.2.1 and 6.2.2) and their preliminary value propositions were updated and shared with the partners, along with the types of exploitation interests and individual exploitation pathways. Feedback received was then used to refine the valorization section.

Following the collection of preliminary data, an initial ownership proposal was created (see Section 6.3.1). This proposal is intended to initiate a discussion within the consortium to ultimately decide on a definitive ownership structure for each project result, whether exclusive or collective. Initially, each partner's role and contribution to the HORSE project results were outlined during the Grant Agreement preparation and are regularly updated as the project progresses.

The process of determining ownership began with an analysis of the various HORSE engines and the overall system architecture. The scripts and other inputs needed to produce the main ERs listed in this document were identified and categorized. Particular focus was given to the initial KERs, mentioned in the initial GA, that make up the HORSE solution.

To formulate the exploitation and valorization plan, an ad hoc IPR matrix was developed by the IPR manager and distributed to all partners, who were then invited to elaborate on their exploitation interests, specifying the type of exploitation and pathway for each HORSE result, both during and after the project. This matrix also collected vital information regarding the exploitation rights and responsibilities anticipated by each partner for the HORSE results. Additionally, it helped the IPR manager to identify potential inconsistencies or unforeseen claims from specific partners early on, allowing for bilateral consultations and proper justification of claims. This proactive approach helped to resolve potential IP conflicts promptly.

Partners contributing to each result were asked to detail their exploitation interests, categorized as: (i)M: making a product ad selling it, (ii)U: use the project result internally for further development (iii)L: licensing the project result to third parties, (iv) S: providing it as a service and (v) O: other. Finally, the partners are requested to choose the most promising path of the ones they chose. The collected information was organized into the exploitation and valorization plan, which includes the IP proposition for each ER and the exploitation interests and pathways for each HORSE partner.

Each stage of the process involved review rounds with partners, which were integrated into the analysis. Throughout the remainder of the project, the information will be periodically refined to incorporate new data and ongoing discussions within the consortium.

6.3.1 Exploitable Results and ownership proposition

Table 17 presents the list of all HORSE ERs with an exploitation potential and interest together with the main partners that have contributed to their creations as well as partners that had the supporting role to their creation. The related BG and FG IP to each project result is also listed, as well as a preliminary ownership proposition and the most relevant means of protecting each result.

Table 17: HORSE Exploitable Results proposition and IP protection

ER number	Main Partner(s)	Contributing Partners	BG number (related)	FG number (related)	Proposition for ER - Owner (if any)	Relevance for IP protection (if any)
ER1	**8Bells**	8BELLS, EFACEC, UPC MAR, ATOS, CNIT ETI, ZORTE	None	FG4.1	Copyright, Patent or Utility Model	None
ER2	**ETI**	None	None	FG3.1	Ericsson exploitation	None
ER3	**TID / CNIT**	None	BG4.2	FG3.2	Exploitation by TID and CNIT	None
ER4	**UPC**	ETI, NKUA, 8BELLS	None	FG3.4	UPC exploitation	None
ER5	**TUBS**	None	BG5.1	FG5.1	None	None
ER6	**SUITE5**	None	None	FG3.5	Copyright - SUITE5	License fee based on multi-party exploitation agreements between Suite5 and the Party/ies involved in exploitation of results
ER7	**8BELLS**	None	BG 4.1		Copyright	License fee based on multi-party exploitation agreements between 8bells and the Party/ies involved in exploitation of results

6.3.2 Key Exploitable Results and ownership proposition

Table 18 presents the list of all HORSE KERs with an exploitation potential and interest together with the main partners that have contributed to their creations as well as partners that had the supporting role to their creation. The related BG and FG IP to each project result is also listed, as well as a preliminary ownership proposition and the most relevant means of protecting each result.

Table 18: HORSE Key Exploitable Results proposition and IP protection

ER number	Main Partner(s)	Contributing Partners	BG number (ralated)	FG number (related)	Licensing	Proposition for ER - Owner (if any)	Relevance for IP protection (if any)
KER1	ATOS	ALL	None	None	Open	None	None

					source / Apache 2.0		
KER2	TID	CNIT, NKUA, S5, UPC, MAR, ZORTE, STS, 8BELLS	None	None	Open source / Apache 2.0	None	None
KER3	STS	CNIT, ATOS, ETI, ZORTE,	None	None	Open source / Apache 2.0	None	None
KER4	ETI	NKUA, UPC, ZORTE, 8BELLS	None	FG3.1	Ericsson proprietary	None	None
KER5	ATOS	CNIT, ETI, TUBS, NKUA, ZORTE, 8BELLS	None	None	Open source / Apache 2.0	None	None
KER6	CNIT	ATOS, ETI, UPC, ZORTE, 8BELLS	None	FG4.1	Open source / Apache 2.0	None	None
KER7	TID/CNIT	CNIT, TID	BG4.2	FG3.2	Open source / Apache 2.0	None	None

6.3.3 Exploitation Pathway per partner

Table 19 and Table 20 offer the exploitation pathway that each partner is going to follow for their ERs as well as KERs. As the project is not near its completion, the partners' proposed exploitation pathways may be modified within the course of the project for one or more ERs. **As such, the following tables represent only a preliminary expression on the consortium's perception on the exploitation pathways that may be suitable for HORSE results.**

Table 19: ER Exploitation Pathway

ER number	Main Partner(s)	M-Making them and selling them	U - Using them	L - Licence them	S - Providing as a Service	O - Others	Most promising path
ER1	8BELLS	X	X	-	-	-	M
ER2	ETI	X	-	-	-	-	-
ER3	TID / CNIT	-	X	-	-	X	U
ER4	UPC	-	X	-	-	-	-

ER5	TUBS	-	X	-	-	X	U
ER6	SUITE5	-	X	-	X	-	S
ER7	8BELLS	X	X	X	-	-	M

Table 20: HORSE KER Exploitation Pathway

ER number	Main Partner(s)	M - Making them and selling them	U - Using them	L - Licence them	S - Providing as a Service	O - Others	Most promising path
KER1	ATOS	-	X	-	-	-	U
KER2	TID	-	X	-	-	X	U
KER3	STS	-	-	-	X	-	S
KER4	ETI	X	-	-	-	-	M
KER5	ATOS	-	X	-	-	X	U
KER6	CNIT	-	X	-	-	X	U
KER7	TID / CNIT	-	X	-	-	X	U

7 Individual Exploitation Plans

The consortium strives to optimize both the technical and economic benefits of the project, ultimately enhancing the value of the invested resources. Leveraging its diverse composition, the consortium will tailor the exploitation of results based on the type of partner involved: industrial entities, clustering organizations, telecommunications companies, Small Medium Enterprises (SMEs), digital technology providers, and end users.

To implement comprehensive and asset-specific exploitation strategies, HORSE will formulate both individual and collective exploitation plans. This chapter focuses on the preliminary exploitation strategies for each partner, documenting the updated interests and expectations of each consortium member, now that the project has been underway for several months.

7.1 Industrial, clustering and telco partners

ATOS: ATOS is a global leader in digital transformation with 109,000 employees and annual revenue of € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the group provides tailored end-to-end solutions for all industries in 71 countries. A pioneer in decarbonization services and products, ATOS is committed to a secure and decarbonized digital for its clients. The purpose of ATOS is to help to design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. ATOS Research & Innovation department (ARI) is the R&D pillar of emerging technologies and source of innovative ideas coming from EU and national funded projects in the organization. Replicating the global organization of the company and with the goal of facilitating the integration of research and innovation activities within the Business Units, ARI is divided into industries, being the Telecommunications Media and Technology (TMT) one of them. The technical expertise of the TMT industry revolves around technologies that enable the development of the next generation telco networks, paying special attention to smart network management and orchestration practices in multi-domain scenarios including the security and privacy aspects. In ARI, there are also business consultants that are involved in the projects from proposal time. These consultants hold regular meetings with the different industries in ATOS to be well updated about the company's strategy, the global portfolio, and the partners and customers' demands. On the other hand, these business consultants provide the company insights about the latest European research trends, the projects and consortia the Unit is involved in and the general results coming out from the projects. This way the company ensures the timely detection of internal and external opportunities and, as part of its general strategy, it supports its clients in achieving their digital transformation and gaining competitiveness. In HORSE, ATOS will act as Technical Manager, supervising the overall technical and scientific progress of the project. ATOS will lead WP4 dealing with the development of an AI-assisted human-centric Secure and Trustable Orchestration module for the HORSE platform. Within the context of WP4 ATOS will lead Task 4.4 focused on the development of the orchestrator connectors aiming to unify the orchestration of all the network segments of the 6G architecture. ATOS technical contribution in HORSE is fully aligned with the technological perspective of the TMT industry and for that reason ATOS believes that the results from HORSE will play a vital role to boost the innovation process within the organization and enhance the portfolio of products and technologies offered to its customers.

TID: TID aims to exploit the project research results in Telefónica, with the goal of promoting the achievements and ideas inside the strategic roadmap of the relevant Telefónica business units in Europe and the world. In particular, TID plans to communicate and promote the HORSE results within the Telefonica Group units working in network evolution and management automation and Cybersecurity services (Telefonica Tech). This will include internal proofs of concept, and training, with the goal of making these units incorporate the results to their commercial service offer beyond the end of the project. In parallel with these actions towards commercial exploitation, other initiatives will also be undertaken. Internal evangelization, through the dissemination of the main project results, across the entire organization, using Telefónica Excellence School, internal communication channels (workplace, ThinkBig blog, etc.), Telefonica Design Councils and TID demonstration rooms. Presentation of the main innovations developed in the project to the entrepreneurship initiatives of Telefonica (Wayra and Telefonica Open Future) with the goal of facilitating their application by the start-ups nurtured by these initiatives. Contributions to standardization bodies (ETSI, IETF, ONF, 3GPP) and EC initiatives (6G-AI, Cybersecurity PPPs, and other future initiatives), whenever applicable. TID is interested as well in possible patents for the services and system pieces derived from the HORSE and in influence on standards and on the development of new related commercial solutions. For these goals, the HORSE concept consolidation is considered a key aspect in providing protection for future 6G network systems deployments. Parallel to these exploitation objectives, TID plans to involve its industrial partners in the security community and stakeholders in the design of technically feasible and scalable commercial products from the above concepts and then cooperate in the transfer process to the industry.

As the research branch in Telefónica, TID aims to exploit project outcomes interacting with its business units' strategic roadmaps. TID is interested in possible patents, in the services and system pieces derived from the HORSE results, and in influence on standards to support the development of new related commercial solutions in the area of network cybersecurity management and automation. Concretely, the module we are responsible for, the Impact Analysis Digital Twin, is the main research activity we want to boost in the HORSE project. Jointly with other partners, as CNIT and UMU, we have contributed to some congress and paper, providing the latest developments in this field.

EFACEC: EFACEC is continuously improving its portfolio solution being more innovative, driven by technologic and being more competitive. The research to be developed in the framework of this project, align with internal roadmap strategy, will have a strong impact in EFACEC's Management and Operation platforms by the validation of proof of concepts and future integration of new technologies such as security, secure and proactive orchestration, AI/ML, edge computing or cloud-native, leveraging to improve its portfolio with better services, with more efficient applications and more resilience platforms.

As an industrial partner, EFACEC aims to maximize the know-how and the advantages of using the 5G/6G technologies, in particular the achievements of the HORSE project, for progressively introducing these new capabilities in its own portfolio for the Metro-Rail market segment. Using 5G/6G wireless solutions to support Metro operations, replacing optical and tetra networks by a single common wireless solution, will be a reality in the near future with an added value of resilience and smart security innovative capabilities.

Adopting a solution, similar to HORSE project, can lead, in the future, to a unique network to support Metro/Rail operations, improving the convergence, integration, the resilience, and the level of security, benefiting from the cost reduction of maintenance and even the CAPEX of a Metro/Rail solution, assuring also the capability to support new type of services.

Therefore, EFACEC is contributing to the HORSE exploitation and dissemination activities through face-to-face client meetings (infrastructure owners and Metro Operators), promoting workshops, participating in conferences and in international events such as InnoTrans, a Trade Fair for Transport Technology.

Additionally, it is also an expectation, to demonstrate to relevant clients and stake-holders, the achievements of HORSE project's, mainly regarding Use Case 1 (Secure Smart Light Rail Transit Systems).

ETI: From the ERICSSON perspective, potentially HORSE will demonstrate to be an innovative framework that differentiate itself from other implementations available on the market and therefore the possible integration of the HORSE system or sub-systems into the Ericsson OSS portfolio could help to gain a competitive advantage over competitors that will likely translate in positive economic repercussions. Moreover, it is important to comment the fact that, besides the aforementioned aspects and their hopefully positive consequences on the Ericsson market with their employment impacts, the competences acquired during this project will contribute to a significant increment on the specialized skill levels of the research groups that will be involved in the different activities; this fact will allow Ericsson to propose itself as a reference partner in future EU projects. All these aspects will provide an important pulse to the R&D activities in this specific emerging technological scenario, with, in turn, an increasing number of applied resources.

The Ericsson DEME (Detection and Mitigation Engine), in this context, represents an innovative and refined Machine Learning based threat module that is under careful consideration for market opportunities. With reference to the Ericsson Business Decision Model, and to the business decisions opportunity evaluation and prioritization, a number of activities have been, or are going to be, put in place comprising technical evaluations and customer feedback collections. For what concerns this latter point, after the second iteration, achieved the complete solution maturity, it will start to be presented in world-wide international Ericsson innovation events, involving hundreds of visitors and tens of telco providers and other relevant customers.

7.2 Academic and Research Partners

CNIT: Within the HORSE project, CNIT will mainly work on the definition of digital twins for 6G networks and the development of the end-to-end secure proactive orchestrator. Based on such assets, the exploitation of the results of the project will go along three lines:

- The primary goal of the exploitation plan of CNIT will be to educate future researchers on 6G and related topics covered by HORSE. The knowledge and results obtained in the project will be used to train young researchers at doctoral and postdoctoral level and to build the next generation of research professionals on those subjects. In particular, several topics and results developed within HORSE will be used to build teaching material, especially at Master and PhD level.
- The development of the orchestrator will enable the CNIT S2N Laboratory to enhance the functionalities of the testbed in Genova and to use it in other projects related to 5G/6G testing.
- The network digital twin developed by the CNIT Research Unit in Trento will represent a relevant asset to open new research lines and to further investigate the topic in research and development activities. Indeed, the network digital twin developed in HORSE will be synergetic to other initiatives in research and education, as well as technology transfer.

As an academic partner and coordinator of the project, CNIT will contribute to the HORSE project's exploitation plans by training B.Sc./M.Sc. students and Ph.D students with state-of-the-art technologies relevant to the future generation of mobile networks. The knowledge gained during the project will be used to enrich the academic offer in the CNIT sites involved in the project, and in particular University of Trento and University of Genoa.

Another exploitation activity will involve participating to the project dissemination activities via publications in international conferences, workshops, and peer-reviewed journals, focusing on advancing technology related to 6G mobile networks. This is already demonstrated by several publications on top-level international journal and conferences, as well as in the organization of dedicated workshops (for example, one workshop is being organized in conjunction with IEEE ICC 2025).

In addition, the CNIT team is active in several standardization working groups, and it is actively pushing HORSE-related technologies within ETSI and other standardization organizations. For example, the concept of Network Digital Twin was recently included in the white paper produced by ETSI ENI, due to the successful discussions on the architecture proposed in this project.

TUBS: TUBS will work on the HORSE platform's architecture, particularly the intent-based modules, which are activities that need our existing knowledge and tools. TUBS will also work on developing new tools, which will likely result in new IPR and scientific discoveries. The tools developed during the HORSE project will be made available as open-source software, facilitating knowledge transfer and collaboration with other research and education actions.

As an academic partner, TUBS expects to contribute to the HORSE project's exploitation plans by training young professional and Ph.D. students with state-of-the-art technologies relevant to the future generation of mobile networks. The knowledge gained during the project will be transmitted to the internal team and students, training them with up-to-date and innovative technologies that 6G networks will employ. Furthermore, TUBS will contribute to the project dissemination activities via publications in international conferences, workshops, and peer-reviewed journals, focusing on advancing technology to support the next generation of mobile networks. In fact, TUBS has already contributed, along with other partners in the HORSE project, to authoring high-impact publications to share the knowledge gained during the project. TUBS will also participate in demonstrations, conferences, and workshops to present the HORSE Project's findings and foster collaboration with industrial partners.

NKUA: NKUA foresees three important routes towards exploitation of the results. The first focuses on exploiting HORSE results in education; the second focuses on enriching the scientific status of the involved personnel; and the third one is aimed at exploiting the project outcomes in future research projects. On the first exploitation strand, HORSE will help extend the undergraduate and MSc courses, while introducing new research topics on the field of 6G security and secure orchestration of highly demanding applications with AI/ML approaches, for the creation of modern and innovative PhD Dissertations. The undergraduate and graduate curricula will be updated and enhanced with new courses on AI/ML-aided cyber-security and will also be enriched through the injection of cutting-edge material from HORSE. In addition, the knowledge gained in HORSE will be leveraged in publishing scientific papers in peer-reviewed journals and venues, maximizing the project's impact. With respect to the second exploitation strand, NKUA sees the participation in HORSE as a clear step towards the exploitation of the technical and scientific advancements, which will be developed in close collaboration with the rest of the project partners. The interest is mainly focused in the areas of physical layer security and AI where

the involved personnel have a remarkable research record and relevant publications. Thus, the participation in HORSE will help the faculty to further strengthen its position in the relevant competitive research areas. Finally, with respect to the third exploitation field, NKUA will leverage the outcomes of this project and build upon the gained expertise to be exploited in new research projects that would give the opportunity to further promote research in these areas. By expanding industrial cooperation with important stakeholders inside Europe, the research findings of HORSE related to AI/ML models, cyber-security and mitigation measures will also be leveraged. The NKUA involvement in a highly innovative project with industrial partnerships will allow its establishment as a significant European research and development organization and it will increase the visibility, recognition, and publication record of the University. Therefore, NKUA will stay competitive for future research projects and initiatives and strengthen its position as a university (knowledge, scientific quality, facilities). Finally, NKUA plans to organize a dissemination seminar with the participation of students from the Departments of Ports Management and Shipping and Digital Industry Technologies of NKUA towards the end of the project.

UPC: UPC's exploitation plans focus on transferring the knowledge gained through the project efforts into the different academic activities involving the team, ranging from undergraduate and master's programs to PhD level education. The main objective is to translate the skills inferred from the project into knowledge to be transmitted within the different courses for undergraduate and master students, while also attracting new candidates to the Computer Architecture PhD program. These candidates will benefit from incorporating distinct concepts from the HORSE project into their training curriculum. This initiative will not only enhance students' knowledge and skills but also significantly increase the team's visibility in the specific areas of the HORSE project where the UPC team contributes. Furthermore, the development of a B5G testbed at CRAAX premises, will undoubtedly open new opportunities for exploitation. These opportunities will be supported by activities such as designing and testing innovative solutions, conducting training in 5G/6G technologies, etc.

In addition, UPC will actively contribute to the dissemination activities by authoring scientific papers and publishing them in recognised international journals, as well as presenting findings at prestigious international conferences and workshops. In doing so, UPC will share the research conducted within HORSE with the global scientific community. Specifically, UPC in collaboration with other HORSE partners, as ATOS, CNIT, NKUA, TID and TUBS, has contributed to journal and conference papers, advancing research in 6G security.

UMU: UMU's primary contribution to the HORSE project has been the deployment of a 5G infrastructure featuring multiple components, such as distributed User Plane Functions (UPFs) and a network of User Equipments (UEs), creating a realistic environment for testing and research. This setup enables the on-demand generation of large volumes of 5G traffic, replicating both user profile scenarios and potential attack vectors for Smart Monitoring. To address 5G-specific threats, UMU has developed an orchestration framework that dynamically manages security policies and applies mitigations on this infrastructure or within a Network Digital Twin (NDT) provided by TID. The framework's key components include a Policy Framework for policy translation and management, a System Model for comprehensive infrastructure modeling, and a Security Orchestrator for executing mitigation actions. This integrated approach demonstrates the practical application of security policies in real-world 5G environments, advancing the state-of-the-art in network security and enhancing resilience against emerging threats.

Building upon the results achieved, UMU plans to further develop and promote this framework in future research and industrial collaborations. The 5G infrastructure and

Network Digital Twin established during the project will serve as foundational platforms for exploring advanced security mechanisms in 5G and future 6G networks. UMU aims to integrate these outcomes into academic research by attracting new talent to PhD programs and fostering collaborations with industry partners and European research initiatives to scale and validate the orchestrator in diverse operational environments. Dissemination efforts will continue through high-impact publications, workshops, and open-source contributions, ensuring that the innovations developed in HORSE leave a lasting impact on both academic and industrial communities.

7.3 SMEs

S5: Suite5 Data Intelligence Solutions (S5) aims to acquire further technological and innovation know-how related to 5G/6G domain, complementing its existing portfolio of data-driven and AI-powered intelligence tools and services. Through its contribution to HORSE activities, S5 plans to experiment with and implement advanced encryption, anonymization, and data observability techniques, further enhancing the capabilities of the S5 Enterprise Analytics software.

As a full member of 6G-IA, S5 is particularly focused on developing AI-based services tailored for network providers. The exploitation of results and insights gained through the HORSE project will enable the company to identify emerging innovation areas and business models relevant to 5G/6G networks, especially those leveraging AI technologies. This knowledge will allow S5 to upgrade its services portfolio with cutting-edge 5G/6G-specific technological advancements.

In addition, S5 will actively promote the knowledge and innovations generated during the HORSE project. This will be achieved through participation in conferences, demonstrations, and workshops, where project findings will be showcased to industry stakeholders. By engaging with key players in the industry, S5 aims to foster collaboration, disseminate best practices, and contribute to the broader impact of the innovations and outcomes produced by the HORSE project. Such activities will not only enhance S5's visibility as a prominent player in data-driven, AI-poweredAI-powered solutions, but also put the company in a position to capitalize on the emerging opportunities within the 5G/6G ecosystem.

ZORTE: ZORTE provides solutions for network virtualization, cloud infrastructure and advanced networking schemes and Internet applications. Main focus areas are Cloud Computing, Remote Sensing applications, Open Programmable Networks, and QoS/QoE provisioning. Therefore, ZORTE expects to obtain significant insight from the results of HORSE, which will reinforce the company's position in the communication and networking field through the upgrade of existing software solutions through hardware acceleration VNFs operating at HORSE network level. Specifically, by participating in this project, ZORTE aims to understand, evolve and exploit its existing hardware acceleration software for virtualized usage. This will enable the capacity of transforming the company's current line of business applications in the field of networking to 6G-enabled solutions.

ZORTE will focus on leveraging the HORSE project outcomes to advance research and development in network slicing and secure orchestration within 6G ecosystems. By concentrating on the Katana Slice Manager, ZORTE will contribute to enhancing the understanding and functionality of network slicing technologies, particularly in the context of dynamic, multi-domain, and highly secure 6G environments. The Katana Slice Manager will be positioned as a research tool to demonstrate advanced capabilities, such as intent-based orchestration and real-time slice monitoring, enabling researchers to explore innovative

solutions for scalable and adaptive network management. ZORTE will collaborate closely with HORSE partners to validate the Katana Slice Manager in real-world scenarios, such as secure operations in light rail transit systems and extended reality environments for industrial collaboration. These use cases will serve as benchmarks for advancing the scientific understanding of secure, efficient, and resilient service orchestration. Furthermore, ZORTE aims to contribute to the academic and research community through publications, participation in international conferences, and collaboration on standards development. By integrating the project outcomes with open-source initiatives, ZORTE will ensure the HORSE project's results contribute to the broader scientific advancement of 6G technologies.

EIGHT BELLS: EIGHT BELLS leverages on the introduction of successful, open-source software stacks for telecom networks that use AI solutions. The participation of EIGHT BELLS in the HORSE project is fully aligned with the company's strategic decision to investigate and to focus on market research about the 6G security telecom segment. In this context, EIGHT BELLS is interested in HORSE outcomes through enhancing the technology and economic enablers in Europe and internationally. The main exploitation actions will be based on obtaining significant insight from the results of HORSE, reinforcing the company's position in the 5G/Beyond5G fields through the upgrading of existing security and software solutions and specialized market reports. This will help to reinforce the company position through contacts with potential stakeholders.

In the context of HORSE EIGHT BELLs is heavily involved in the development of tools crucial to HORSE's workflow. The two modules EIGHT BELLS is responsible of, are the Pre-processing and the Reliability Trust and Resilience modules. Both of those components provide EIGHT BELLS with the opportunity to foster the growth of its research and innovation capabilities. More specifically:

- The Pre-Processing component is designed to enhance the integration and management of data streams from diverse and heterogeneous sources. 8BELLS will emphasize its adaptability and effectiveness by organizing targeted demonstrations that highlight its ability to integrate data from IoT sensors, relational and non-relational databases, and deliver pre-processed outputs to user-defined endpoints, such as APIs. These demonstrations will engage key stakeholders, including critical infrastructure operators and organizations navigating complex network ecosystems. Additionally, 8BELLS will actively participate in conferences, workshops, and webinars to illustrate the component's capability to streamline data flows and foster interoperability across varied applications. Insights from early adopters will be meticulously collected and analyzed to refine the component's functionalities and address emerging demands. Future efforts will focus on forming strategic alliances and exploring licensing models to drive the widespread adoption of the Pre-Processing component, enabling it to play a pivotal role in advancing data handling and interoperability in heterogeneous network environments.
- The RTR component, on the other hand, showcases its transformative potential in simplifying and optimizing the management of next-generation network environments. By offering an API capable of translating threat mitigation requests from physical language into actionable commands, the RTR component allows operators to implement their intentions with significantly reduced effort and time. 8BELLS plans to highlight its practical value through tailored demonstrations targeting network operators and cybersecurity organizations, showcasing its ability to streamline threat response workflows. Participation in industry events such as conferences, webinars, and workshops will further amplify the RTR component's visibility and emphasize its novel approach to intent-driven network management. Feedback from early adopters will be

systematically gathered to enhance the component and adapt it to evolving user requirements.

MARTEL: MARTEL has identified several ERs from the HORSE project that will be instrumental in enhancing the security features of Martel commercial IoT platform, Orchestra Cities. Specifically: i) Knowledge Base (KB): Developed internally, this database is crucial for accumulating and sharing security-related information across the platform. ii) Attack/Mitigation Service: Also developed in-house, this service is designed to offer an interface for obtaining mitigation solutions. iii) Ansible Playbooks: developed by external parties, our contributions will enhance their utility and integration within the systems. iv) valuable knowledge acquired during implementation, essential for ongoing development and refinement processes.

The technical work within HORSE will support the activities of MARTEL in this area by exploring the adoption of AI based solutions, strengthening its commercial credibility and overall reputation in the SNS JU context and beyond in the European and worldwide 6G context. Moreover, the impact creation activities performed in HORSE are expected to increase visibility and expertise of MAR, which are key to create new collaboration and business opportunities with top players in the Telco scene.

MARTEL aims to maximize the impact of the project through strategic dissemination and communication activities. This includes publishing scientific articles and presenting research findings through renowned international journals and conferences, ensuring that the cutting-edge advancements from the project reach and benefit the global scientific community. Key results will be showcased into workshops and training programs, complemented by the sharing of open-source code and detailed documentation to ensure accessibility and transparency of the project's findings, for broader adoption and collaboration in the community. Additionally, MARTEL will keep the HORSE website and social media up to date, will share findings and highlight the participation of HORSE's partners in conferences and presentations, while scientific articles and news related to the project will also be made available online to enhance visibility.

The HORSE project will also generate exploitable results that will directly benefit MARTEL's commercial IoT platform, called Orchestra Cities. These ERs include the development of a Knowledge Base (KB) for consolidating and sharing security-related information, an in-house Attack/Mitigation Service that provides an interface for obtaining mitigation solutions powered by Generative AI. Additionally, the technical work in HORSE supports MARTEL's exploration of AI-based solutions, augmenting the Orchestra Cities' capabilities and strengthening the company's reputation within the SNS JU framework and the broader 6G landscape. The visibility and expertise gained through the project, especially in the field of Artificial Intelligence and, in particular, Generative AI, are expected to create new collaboration and business opportunities with leading players in the telecommunications industry.

HOLO: By joining HORSE Holo-Light will leverage its expertise in visualizing, interacting, streaming XR content in order to improve the performance and versatility of its products and make them "6G ready" also to address the future B2C market.

As an augmented reality software company specializing in XR streaming solutions, HOLO recognizes the importance of robust, efficient, and secure network infrastructures for its operations. Consequently, HOLO is committed to validating and leveraging the outcomes of Project HORSE while ensuring their wide dissemination and practical application.

- Facilitating Knowledge Sharing and Collaboration: HOLO is dedicated to promoting the dissemination of the innovations and knowledge generated by the HORSE

project. By acting as a knowledge broker, HOLO will share insights and results with stakeholders in the critical infrastructure sectors across local and European levels. This initiative aims to foster collaboration, encourage the adoption of advanced cybersecurity solutions, and support the implementation of safer network infrastructures in industries that rely on these technologies.

- Engaging Industry Partners through In-House Events: HOLO will leverage its regular in-house events as platforms to highlight the outcomes of Project HORSE. These events, tailored for key industry partners, will demonstrate how the project's results align with real-world applications and address pressing challenges in XR streaming and broader industrial contexts.
- Showcasing Results at Conferences and Workshops: HOLO plans to actively participate in industry conferences, demonstrations, and workshops. By presenting the findings and innovations from the HORSE project, HOLO will engage with leading industry players, fostering meaningful discussions and partnerships. This outreach will ensure the project's outcomes gain visibility and recognition, contributing significantly to the advancement of secure network technologies.

STS: The exploitation strategy for Smart Monitoring (KER3) centers on several key actions to ensure its relevance and widespread application beyond the HORSE project. To begin with, STS will organize detailed demonstrations to highlight KER3's ability to collect and analyze diverse data streams, detect anomalies, and strengthen cybersecurity in 5G/6G ecosystems. These showcases will be directed at critical stakeholders, including telecom operators, cybersecurity firms, and entities managing essential infrastructure, to illustrate its robustness and practical value. Outreach initiatives will also include active participation in industry conferences, hosting webinars, and publishing articles or case studies to communicate the advantages of KER3 effectively.

STS has been developing a product suite to support enterprises in setting up and continuously monitoring, assessing, and managing security and privacy risks to their assets, and overall, their business – including ICT infrastructures, applications, data, and processes – from both a technical and a business/economic perspective. At the core of this offering lies the security and privacy (S&P) assurance platform, which was deployed and run in support of HORSE project's use cases, and offers a comprehensive solution for cyber security assessment.

STS plans to offer its product suite through different subscription-based managed security services (MSS) that can be tailored to the needs of its clients (e.g., for hybrid or cloud-based deployments, different subscription tiers). The product suite of STS and the services that we are planning to offer address specific sectors of the CSPS market: application security, infrastructure security, situational awareness, business continuity, and cyber consultancy.

A more precise indication of the exact types of products/services within the above sectors, which are addressed by SPHYNX's products and services is given in a study (Cybersecurity industry market analysis, https://op.europa.eu/en/publication-detail/-/publication/0be963c5-ca06-11e9-992f-01aa75ed71a1) for the CSPS market (where SPHYNX will primarily operate).

8 Market Analysis

The launch of fifth generation (5G) wireless technologies marked a significant leap in telecommunications, enabling unprecedented speeds and connectivity, hence enabling new applications of both consumer and industrial nature. However, full coverage and optimization of 5G networks are still works in progress, accompanied by a gradual shift towards the next frontier: sixth generation (6G) mobile communication. While the 6G standardization process is projected to commence around 2026, a vibrant research community has already begun to explore innovative pathways to realize this next generation of telecommunications.

6G is envisioned not merely as an extension of 5G, but as a transformative architecture that incorporates entirely intelligent orchestration and management of networks [4] [5]. This forward-thinking framework is anticipated to leverage multiple cutting-edge technologies, including Internet of Everything (IoE), and quantum computing, among others [6]. The evolutionary trajectory of 5G, which has introduced mechanisms like virtual radio access networks (vRANs) and cloudified core networks, forms the foundation upon which 6G will be built.

8.1 5G/6G networks security and cybersecurity market

According to currently available studies and forecasts, the 6G market is anticipated to grow at a Compound Annual Growth Rate (CAGR) of 76.9% from USD 3.96 billion in 2030 to USD 98.69 billion by 2035. In the meantime, and as cyber dangers evolve, 6G networks are being developed with enhanced security measures to safeguard data and communications from hackers. Those networks are anticipated to utilise AI to detect and mitigate attacks in real-time, therefore safeguarding critical information and infrastructure from being compromised. Also, it is expected to implement quantum-resistant encryption to safeguard against prospective dangers posed by advanced quantum computers. Moreover, 6G will strengthen all network levels, ensuring comprehensive end-to-end security [7].

Regarding the 5G security market, it is expected to grow from 1.7 billion USD in 2023 to 9.2 billion USD by 2028, with a compound annual growth rate of 38.9% between 2023 and 2028 [8]. The industry is growing as cyberattacks become more sophisticated, targeted, and difficult to defend against. As cyberattacks get more sophisticated, firms must invest in stronger security measures to protect themselves. This entails investing in emerging security technologies like AI and ML, as well as training personnel on proper security practices.

According to [9], the cybersecurity market size is estimated at USD 182.84 billion in 2024, and is expected to reach USD 314.28 billion by 2029, growing at a CAGR of 11.44% during the forecast period (2024-2029). The rising number of cyberattacks worldwide and the increasing digitalization have the potential to harm the internet-linked digital infrastructure of numerous government or private sector enterprises, which would greatly accelerate the market growth rate. These are the main factors driving the adoption of data-intensive and automated approaches.

8.1.1 Market impact factors

HORSE focuses a lot on safeguarding 5G and future 6G services. The industry is growing as cyberattacks become more sophisticated, targeted, and difficult to defend against. As cyberattacks get more sophisticated, firms must invest in stronger security measures to

protect themselves. This entails investing in emerging security technologies like AI and ML, as well as training personnel on proper security practices.

Factors that directly or indirectly impact the market were analysed to estimate the overall trend of the market during the forecast period (Table 21). Each factor was analysed on a scale of 1–3, 1 being the lowest and 3 being the highest [8].

Table 21: 5G/6G security market impact factors

Factor	Inference	Impact
Recent Developments	Partnerships, new product releases, and product updates are primarily driving the 5G/6G security market. The major suppliers account for 80-90% of market advancements. As a result, this factor will have a significant market influence.	High
Enterprises' 5G Spending	Over the last few years, corporations have increased their investment on private wireless networks and 5G/6G network infrastructure, particularly large and medium firms. Organizations are embracing new technologies to improve business processes and increase revenue. Digital transformation programs have aimed to encourage businesses to boost their capital expenditure on network and development infrastructure. As a result, this element will have a significant market influence.	High
Regulations	Regulations have an indirect impact on the 5G/6G security industry. There are numerous rules that do not have a direct impact on the 5G/6G security industry. As a result, this factor will have a medium impact on the market.	Medium
Technology Maturity	The 5G/6G security market is still in its early stages of development and is predicted to grow. The adoption of IoT, AI/ML, and the cloud is projected to drive the 5G/6G security market in the coming years. As a result, this factor will have a medium impact on the market.	Medium
Mobile and Internet Penetration	North America and Europe have the highest percentages of mobile and internet penetration. In terms of mobile and internet penetration, Asia Pacific, the Middle East and Africa, and Latin America all offer considerable growth prospects. This encourages enterprises to use 5G security solutions and services to protect their 5G/6G networks. As a result, this factor will have a medium impact on the market.	Medium
Mergers and Acquisitions (M&A)	There have been few 5G/6G security market acquisitions over the last few years. As a result, this element would have a minimal impact on the market.	Low

Startup Ecosystem	The 5G/6G security market is dominated by established manufacturers such as Cisco, Huawei, Ericsson, ZTE, and Palo Alto Networks. Few startups operate in the 5G/6G security market. As a result, this element would have a minimal impact on the market.	Low

8.1.2 Market Trends

8.1.2.1 Development of network security and protection tools

Network security is essential for safeguarding computer networks and systems against unauthorised access, abuse, and disruption. Attackers can bypass traditional techniques, requiring the deployment of artificial intelligence (AI) and machine learning (ML) instruments to detect emerging threats and adjust to evolving assault methodologies. Behavior-based intrusion detection is a widely utilised artificial intelligence technique for network security [10]. These systems utilise AI algorithms to evaluate and categorise network traffic according to its behaviour. Also, they are capable of learning the typical behavior of a network and using that information to find and categorise abnormalities. These anomalies can subsequently be analysed to detect possible cyber-attacks [11]. Another widely utilised technique for enhancing network security is unsupervised learning, a method within the realm of AI. Unsupervised learning methods, like clustering and anomaly detection, are utilised to identify patterns in network data that diverge from typical behaviour. These algorithms can detect previously unidentified cyber-attacks by clustering analogous network traffic and recognising any communication that is anomalous to the group. ML techniques, particularly reinforcement learning, are extensively employed in network security. Reinforcement learning algorithms specifically enhance the functionality of network security systems. Through a trial-and-error process, these algorithms learn from the consequences of their activities, therefore increasing the decision-making abilities of network security systems [12].

8.1.2.2 Zero Trust Framework

Zero trust is a security model for modern multicloud networks. A zero-trust security model prioritises the enforcement of security regulations for each distinct connection among people, devices, applications, and data, rather than concentrating on the network perimeter. Zero trust is based on the philosophy of "never trust, always verify," instead of automatically trusting all users inside a network. This sophisticated security strategy mitigates the cybersecurity threats associated with remote employees, hybrid cloud services, personal devices, and other components of modern corporate networks. A growing number of organisations are implementing zero trust models to enhance their security frameworks as their attack surfaces expand. A 2024 report by TechTarget Enterprise Strategy Group [13] indicates that over two-thirds of organisations are adopting zero trust policies throughout their enterprises.

A zero trust approach is essential as the conventional concept of network security is inadequate. Zero trust techniques are formulated for the intricate, extensively distributed networks prevalent in contemporary organisations. For several years, organisations concentrated on safeguarding the boundaries of their networks using firewalls and various security measures. Individuals within the network perimeter were deemed reliable and had unrestricted access to programs, data, and resources.

Digital transformation eliminated the traditional idea of a network perimeter. Currently, corporate networks encompass areas beyond on-site locations and network segments. The modern enterprise ecosystem encompasses cloud environments, mobile services, data centres, IoT devices, software-as-a-service (SaaS) applications, and remote access for employees, vendors, and business partners. The expanded attack surface makes organisations increasingly susceptible to data breaches, ransomware, insider threats, and various forms of attacks. The network perimeter is no longer a solid line, and perimeter-based defences cannot bridge every gap. Furthermore, threat actors that infiltrate a network might exploit implicit trust to execute lateral movements in order to identify and target essential resources.

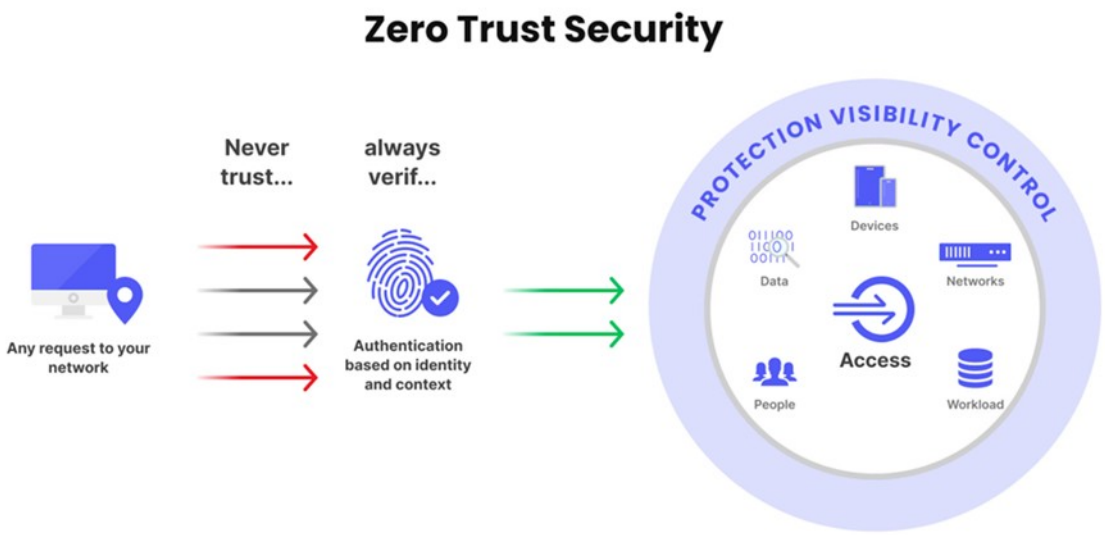


Figure 16: The zero trust architecture [14]

The technical specifications of different frameworks and models can vary, but they all follow a core set of zero trust principles [15]:

- **Continuous monitoring and validation:** Zero trust makes all network assets inaccessible by default. Users, devices, and workloads are required to undergo continuous, contextual authentication and validation to access resources, necessitating these checks with each connection request.
- **The principle of least privilege:** In a zero trust framework, users and devices possess minimal access privileges to resources. This indicates they obtain the essential degree of authorisation necessary to execute a job or perform their duties. The permissions are revoked upon the conclusion of the session.
- **Assume breach:** In a zero trust organisation, security teams operate under the assumption that hackers have already infiltrated network resources. Measures employed by security teams to alleviate an active cyberattack become regular operational procedures. These measures encompass network segmentation to restrict the extent of an attack; continuous monitoring of all assets, users, devices, and processes within the network; and immediate response to anomalous user or device behaviours.

HORSE leverages advanced data monitoring technologies to secure critical 5G/6G infrastructure against increasingly sophisticated cyber threats. By capturing and analyzing traffic data (e.g., NGAP/NAS-5GS, GTP-U, PFCP), it enables the detection of vulnerabilities such as unauthorized access to network slices, anomalies in data flows, and potential breaches across software-defined architectures. Modern 5G/6G security demands focus on

zero-trust frameworks, real-time analytics, and enhanced visibility into network activity. HORSE fits seamlessly into these trends by collecting data from diverse sources, converting it into actionable insights using tools like tshark and Elasticsearch, and enabling near-instantaneous responses to potential threats. This aligns with the growing need for proactive threat detection, lifecycle security, and resilience in distributed, cloud-native 5G/6G environments.

8.1.2.3 Expansion of IoT towards IoE

The increasing deployment of Internet of Things (IoT) devices, along with the surging popularity of cloud computing, is enhancing market growth. IoT devices provide increased convenience and efficiency, enabling users to remotely manage devices, collect real-time data, and automate activities. The swift proliferation of IoT devices is altering the methods of data storage, access, and transmission. Additionally, organisations are investing in robust security solutions, including encryption protocols, identity and access management, and secure communication channels, to safeguard data both in transit and at rest across many platforms [16].

The Internet of Everything (IoE) is an expansion of the IoT that encompasses objects, data, individuals, and processes. The main idea of the IoE is to amalgamate diverse sensing devices associated with "everything" to identify, monitor status, and make intelligent decisions, hence generating new opportunities.

At the core of the Internet of Everything lie four foundational pillars [17]:

- People represent the human element in this interconnected ecosystem, where individuals interact with devices and systems to drive innovation and create value.
- Process refers to the workflows and procedures that govern how tasks are executed and decisions are made within organisations and communities.
- Data is the lifeblood of IoE, encompassing the vast streams of information generated by connected devices and systems, which are analysed to extract insights and drive informed decision-making.
- Things denote the myriads of interconnected devices, sensors, smart grid technology, and machines that form the physical infrastructure of IoE, enabling the seamless exchange of data and communication across the network.

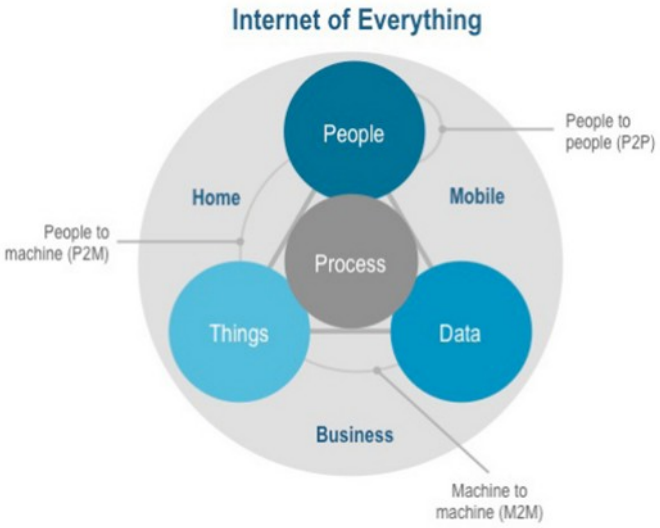


Figure 17: The What, Where, and How of the IoE [12]

Some vital industry sectors have already benefitted from the IoE. In the manufacturing sector, the IoE is facilitated through the implementation of sensors throughout production machinery and equipment. These sensors provide the detection of physical damage (breakdown, erosion) in machinery and quantify the financial loss resulting from such damage. The sensors can provide advance alerts and assist organisations in proactive repairs, allowing for maintenance decisions to be made before conditions become urgent. Consequently, the lifespan of any equipment may be anticipated as IoE-based sensors always monitor its components. Furthermore, timely alerts substantially decrease equipment downtime and maintenance expenses [18].

Given the millions of trucks and boats in transit globally, along with significant opportunities for optimisation across all sectors, the implementation of a distributed network of interconnected sensors and advanced software appears to be a logical approach to enhancing innovation in logistics. IoE enables process enhancements across several locations, including warehouses, sorting facilities, airports, and service stations. The use of sensor arrays and AI-driven port management software at seaports may provide multi-million-dollar savings through the optimisation of docking and loading/unloading operations, predictive repair of equipment, and automation of warehousing procedures [19].

5G/6G is anticipated to serve as a crucial facilitator for the IoE, including extensive machine-type (M2M) communication and sensor devices. The amalgamation of 5G/6G with the IoE would enhance services associated with the Internet of Things, Internet of Medical Things, robotics, smart grids, smart cities, body sensor networks, and several other domains [20]. Nonetheless, the IoE is anticipated to rely on 6G, since it necessitates the capability to link N intelligent gadgets, where N is a scalable word that may extend to billions. Furthermore, the IoE requires elevated transmission speeds to accommodate and enable numerous devices with little latency. Consequently, IoE and 6G may enhance corporate operations by generating vast amounts of data and transforming digitalisation through advanced and rapid data analytics [21].

HORSE provides a unified interface to enforce mitigation actions abstracting from existing infrastructure. The main goal is to achieve the way to enforce actions in a multi environment from just one single entity and also to enforce mitigation action regardless of the infrastructure to facilitate the interoperability through different operators/owners of the network.

8.1.3 Adoption of 5G/6G networks

In this chapter, two ecosystems which are correlated with the HORSE use cases are presented.

8.1.3.1 Smart cities

With the advent of 5G/6G, there is a brighter chance for smart cities to come into effect. 5G/6G offers the necessary parameters for smart cities to connect, including the use of sensors, analytics data, and more. Statista reports [22] that the global IoT in smart cities is expected to grow by 18.8%. 5G/6G is considered the driving for smart cities as it can connect everything from machines, objects to devices better than the existing 4G technology. 5G is already helping cities improve traffic flow and air quality with sensors connected via the IoT, but the future will likely bring much more innovation to this space.

According to IBM [23], one of the biggest areas where smart cities can leverage 5G more is in its AI capabilities. Currently, programs are being tested that would see 5G-enabled AI assist in everything from smarter energy management to the routing of 911 calls. In Vienna, WienBot, an AI chatbot [24], helps users solve problems as simple as finding the nearest drinking fountain or a place to eat dinner to as complex tasks as renewing their passport and obtaining travel visas.

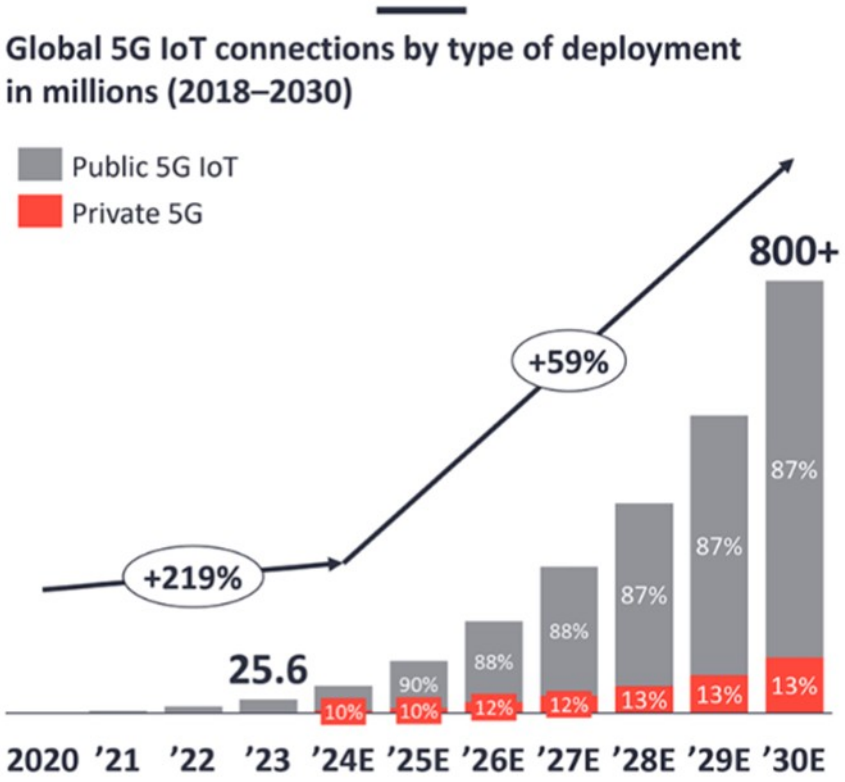


Figure 18: 5G IoT market size [25]

8.1.3.2 Supply chains

Supply chains worldwide will profit from 5G/6G connectivity's lightning-fast speeds and enhanced reliability as it expands. The increasingly digitalised networks that underpin international trade are more dependent than ever on 5G/6G speeds and high-speed data transfer capabilities. As digitisation and automation within a supply chain become more common, the potential for using 5G and 6G technologies to enhance efficiencies, minimise costs, and bolster security consequently increases.

Airports, ports, train stations, and other centres of logistics essential to supply chain infrastructure are already utilising 5G service today, but its full potential has not been realised. 5G and 6G connection will soon be more important in improving the consumer and employee experience. IoT gadgets, such shelf sensors that detect when an item is out of stock and instantly make a new order, cashierless checkouts, HD cameras and drones to take the role of security guards and the use extended reality (XR) in Industry 4.0 among the projects that are already in experimental stages [23].

8.1.4 Stakeholders

Academia & Researchers in Information and Communication Technology (ICT) and cybersecurity: These institutions of learning are leading the way in the field of research and instruction. Their goal is to use the innovations and insights produced by the HORSE project to further their research agenda. They also see a chance to improve workforce and student capabilities by incorporating cutting-edge cybersecurity ideas into their curricula and training initiatives. Additionally, they can help by incorporating the outcomes of the HORSE project into real-world case studies, which will promote a pragmatic grasp of cybersecurity.

Consortia from SU-ICT-02 & other relevant EU-funded projects: Through their participation in HORSE project events and information sharing activities, these groups hope to increase their knowledge. Especially projects from SNS JU, 6G-IA, NetWorldEurope IoT, Cloud, AI and SU-ICT-02 can increase the impact of their own projects and research endeavors by discovering areas of mutual interest and synergies. This partnership may also result in the planning of events together, which would promote innovation and knowledge exchange even more.

EU vendors of security components: These businesses play a crucial role in supplying the market with necessary security components and solutions. They see the results of the HORSE initiative as an invaluable tool to improve their products and maintain their competitiveness. They can build new services and solutions that address changing cybersecurity needs by integrating project results into their operations and R&D initiatives.

ICT developers & integrators: These parties are involved in both the development and application of technology. In order to strengthen 5G infrastructure security, they are interested in combining Horse results with their internal solutions. Through this partnership, they will be able to address the growing demand for secure ICT solutions and access new revenue streams through enhanced and innovative market offerings.

Stakeholders in 5G & telecom industry: These stakeholders are looking for cutting-edge cybersecurity technologies and services to guarantee the reliability of the European Digital Single Market, with 5G technology at the center of the digital transformation. They can improve their security posture and add to the general security and dependability of 5G networks and services by implementing the results of the Horse project.

SMEs and large enterprises in critical sectors: For these organizations, data and secure services are of outmost importance. They could be interested in using the technologies developed for the HORSE project to improve standards and regulation compliance as well as evaluation, inspection, and validation. This way, they could minimize vulnerabilities, safeguard sensitive data, and foster trust with their partners and clients by doing this.

ICT/Cybersecurity agencies; Public authorities, cyber-security, security initiatives, fora and policy makers at EU & national levels: These organizations are essential in forming the cybersecurity regulatory and policy environment. In order to influence future laws and regulations, they are eager to assess the technological and financial effects of the HORSE initiative. The project's conclusions can direct national and EU investment choices as well as research goals.

Investors & Funding organizations: The goal of these stakeholders is to find innovative breakthroughs that have the potential to become profitable ventures. They can help bring cutting-edge cybersecurity technology to market, promoting economic growth and competitiveness, by discovering and supporting Horse project ideas.

ECSO, other relevant Cyber Physical Production Systems (cPPSs), and EU Technology Platforms: In the field of cybersecurity, cooperative research and information sharing are crucial. These organizations want to share the findings of the Horse project with their members and larger stakeholder groups as well as incorporate them into their research endeavors. This partnership encourages novel cybersecurity solutions to be widely adopted.

European and worldwide initiatives such as ENISA, ADRA, AIOTI, BDVA, HPC, GAIA-X, and FIWARE: These will play a crucial role in fostering knowledge exchange and gathering important information about best practices and innovative approaches. Engaging with these initiatives will enhance their awareness of the European and global challenges in the relevant domains, promoting a collaborative understanding. This collaboration will also highlight and disseminate research challenges, best practices, and key research topics, contributing to more informed and effective future design. Through this synergy, we aim to elevate the standards and impact of ongoing and future projects in the field.

Civil society and community at large: Stakeholders interested in the HORSE project, such as community organizations, policy makers, and advocacy groups, will benefit significantly from being informed about project advancements, best practices, and outcomes. Keeping these stakeholders updated fosters transparency and trust, ensuring they are aware of the progress and successes achieved. Regular communication will enable these groups to liaise effectively with HORSE stakeholders, facilitating collaboration and knowledge sharing. Additionally, raising awareness of the social aspects related to the project's activities and solutions can drive community engagement and support, highlighting the project's broader societal impact and encouraging the adoption of innovative practices that address both technical and social challenges.

Standardization bodies and open-source initiatives: These are vital stakeholders for the HORSE project. HORSE partners will actively participate in and contribute to various standardization and open-source initiatives. By doing so, they will ensure that the project's developments align with current standards and open-source practices, fostering greater interoperability and adoption. This involvement will also provide a platform for sharing insights and advancements from the HORSE project, influencing future standards and open-source projects. Engaging with these initiatives will help in promoting the project's outcomes, ensuring they meet industry benchmarks and are widely accessible for broader impact.

8.2 Resilience challenges in 5G/6G networks

8.2.1 Rising incidences of cyber threats and data breaches

Cyber threats encompass several illegal acts, including hacking, phishing, malware attacks, and ransomware incidents. These attacks exploit weaknesses in networks, systems, and software to get unauthorised access, expropriate sensitive information, or disrupt operations. 5G/6G networks, with their high-speed data transfer and interconnected devices, are vulnerable to advanced cybersecurity threats. Therefore, businesses are pursuing security solutions that protect their networks and avert financial loss, reputational harm, and legal consequences. Consequently, firms are investing in sophisticated intrusion detection systems, next-generation firewalls, and threat intelligence solutions to proactively detect and prevent possible attacks. The rising need for network security, driven by the proliferation of cyber threats and data breaches, is propelling market expansion [16].

HORSE has a central control point for its security infrastructure, coordination of actions, monitoring of systems and enforcing security policies. This centralized approach offers efficient management of complex, distributed systems. The HORSE capabilities could also be adapted for external applications. For instance, it could be used to manage security across multiple organizations or to provide advanced security services to third-party clients.

8.2.2 Distributed Architecture and Increased Attack Surface

The distributed design of 5G and 6G networks considerably expands the attack surface, introducing novel cybersecurity issues. 5G and 6G employ a decentralised methodology in which core network services are distributed over several edge nodes. This transition provides operational benefits such as reduced latency, improved scalability, and increased flexibility in service rollout. However, it also creates several possibilities for attacks [26].

In 5G/6G networks, where services are extensively distributed over edge nodes and cloud infrastructures, a Distributed Denial of Service (DDoS) attack aimed at a pivotal node might result in considerable interruptions to essential network services. Given that 5G and 6G networks depend significantly on edge computing to provide low-latency services, especially for applications such as autonomous driving, the effects of a DDoS assault might be disastrous. By focussing on the edge, attackers can interrupt data transmission between devices and the cloud, decrease service performance, or induce whole service disruptions [27]. Furthermore, 6G will enhance dependence on edge infrastructure, resulting in an expanded attack surface for DDoS attacks. It has been underscored that 5G/6G networks require resilient DDoS prevention techniques, encompassing AI-driven traffic filtering, anomaly detection, and adaptive firewalls [28]. These technologies can facilitate the early detection of harmful traffic patterns and alleviate the impact of DDoS assaults. The use of AI and ML can evaluate network data in real time, detecting irregularities that may signify an active assault [29].

Furthermore, the distributed edge computing environment, which positions network services closer to the user, also amplifies the number of possible targets for attackers. An increased number of edge nodes correlates with a greater number of potential vulnerabilities for an attacker to exploit [30]. In contrast to a centralised system, where security management is relatively straightforward, distributed architectures provide difficulties in the implementation and enforcement of uniform security rules across all nodes. Edge nodes may possess varying levels of security or processing capacity compared to centralised cloud systems, rendering them more susceptible to attacks. Should an edge node be infiltrated, an attacker may get access to sensitive data, interrupt services, or enter the wider network. Securing edge nodes necessitates proper configuration, regular updates, and robust access control methods for each node [31].

The advent of 6G technology heralds an era where the IoE will become a reality, with a vast proliferation of low-cost, low-intelligence devices significantly expanding the security perimeter. This massive growth in connected devices introduces a complex landscape for cybersecurity professionals, with potential threats escalating to an unprecedented scale. Alongside traditional cybersecurity challenges, such as DDoS attacks, which will be amplified by the enhanced capabilities of new networks, novel issues are emerging. The threat landscape is becoming increasingly sophisticated with the potential misuse of Generative AI (GenAI) and Quantum Computing, which could further complicate security efforts.

As we advance, network solutions will become more intricate, featuring requirements like personal subnetworks and extreme slicing, and giving rise to new, dangerously potent forms

of attack such as zero-day vulnerabilities. These threats are unique and unknown, making them particularly hazardous. To combat these challenges effectively, innovative cybersecurity solutions are required. HORSE has proposed a groundbreaking approach leveraging ML, especially through a multistage architecture designed to enhance global visibility. This architecture aims to transcend the traditional silos of current security solutions, providing a dynamic framework capable of adapting to and learning from these evolving threats, including elusive zero-day attacks. By embracing this adaptive and innovative approach, cybersecurity frameworks can remain resilient and responsive to the rapidly changing digital landscape.

8.2.3 Quantum Computing

Quantum computing is an emerging domain of advanced computer science that utilises the unique characteristics of quantum mechanics to address challenges beyond the capabilities of the most powerful traditional computers. The area of quantum computing encompasses several fields, including quantum hardware and quantum algorithms. Although currently under development, quantum technology is poised to address intricate challenges that supercomputers are either incapable of solving or cannot resolve with sufficient speed [32].

Quantum computing has theoretical applications in modern computer systems, including cellular networks such as 5G/6G. However, issues around privacy and data security are poised to be crucial as new vendors and technologies develop to leverage 5G/6G capabilities. The expansion and substantial architectural modifications will generate complex networks, revealing new vulnerabilities and increased threats as we transition to a post-quantum (PQ) age.

Quantum computers have the potential to breakdown encryption methods, presenting a considerable risk for modern telecommunications networks. The advancement of quantum-safe cryptography, or Post-Quantum Cryptography (PQC), is an essential priority for Mobile Network Operators (MNOs) to safeguard communications on 5G/6G networks. The advancement of PQC remains immature and is now undergoing standardisation, led by NIST, NSA, and GSMA [33].

HORSE leverages a multistage ML architecture to enhance global threat visibility, which is critical in addressing the sophisticated cybersecurity challenges of 5G/6G networks. By focusing on threats like DDoS attacks and Quantum Computing, HORSE can provide an adaptive framework capable of learning from and responding to evolving threats.

8.2.4 Zero-day attacks

A zero-day exploit is a cyberattack method that targets an unidentified or unresolved security vulnerability in software, hardware, or firmware. "Zero day" denotes that the software or device provider has no time to rectify the vulnerability, since malicious entities can use it to break into susceptible systems. A zero-day vulnerability or zero-day danger refers to an undiscovered or unresolved vulnerability. A zero-day attack occurs when a malevolent entity use a zero-day exploit to deploy malware, exfiltrate data, or inflict harm on individuals, organisations, or systems.

A zero-day vulnerability is present in a version of an operating system, application, or device upon its release, undiscovered to the software vendor or hardware manufacturer. The vulnerability may remain unknown for days, months, or years until detected. Ideally, security researchers or software developers identify the vulnerability prior to its discovery by

malicious actors. Nevertheless, hackers occasionally exploit the vulnerability prior to detection.

Regardless of who discovers the flaw, it often becomes public knowledge soon after. Vendors and security experts generally inform clients to enable them to implement measures. Hackers can disseminate the threat among themselves, while academics can get insights by observing cybercriminal activities. Certain suppliers may hide a vulnerability until they have created a software update or alternative solution, however this approach might be dangerous. If hackers exploit the vulnerability prior to vendor remediation, organisations may be vulnerable [34].

The "HORSE intelligence" working package is pivotal in shaping the platform's cognitive capabilities. From the outset, it has aimed to enhance the capacity to identify zero-day attacks that could pose significant threats within the 5G/6G context, particularly as hackers increasingly utilize machine learning and generative AI techniques to develop new forms of attack. This vital feature, coupled with the robust collaboration of advanced cybersecurity tools and an optimized architectural design, positions the HORSE platform as an attractive prospect in the emerging 5G/6G market.

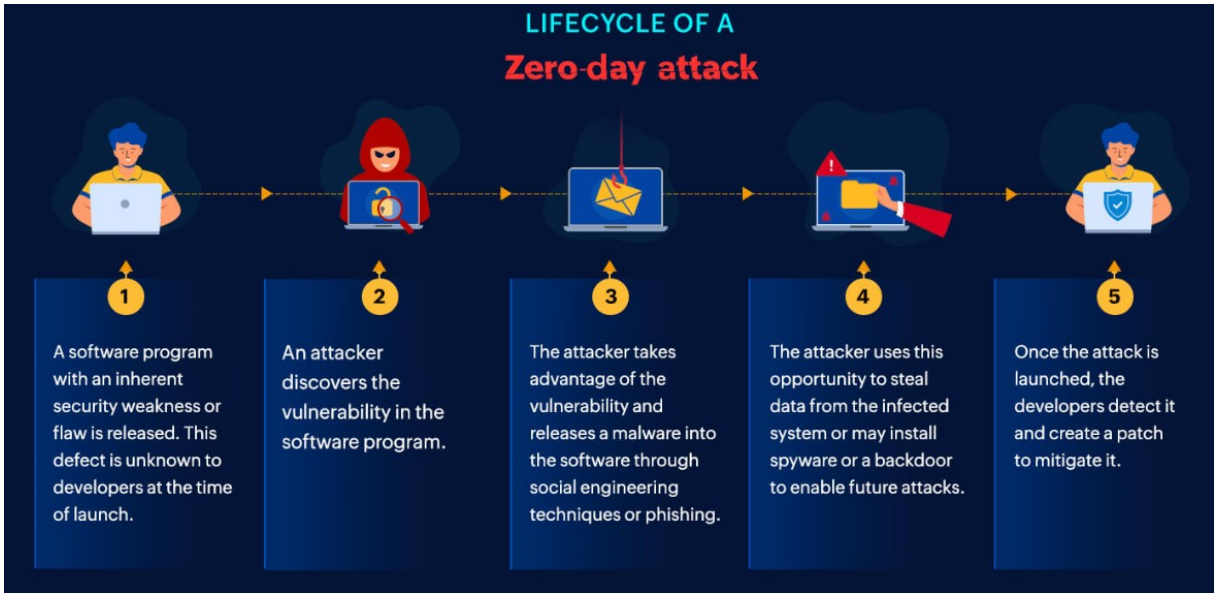


Figure 19: The lifecycle of a zero-day attack [35]

8.3 Advances and trends in 5G/6G networks resilience technologies

8.3.1 Intrusion detection and response

Intrusion Detection and Response (IDR) is an essential part of network cybersecurity, aimed at detecting and addressing possible attacks prior to inflicting harm on computer systems [36]. Historically, IDR systems have depended on rule-based and signature-based methodologies, which may inadequately identify novel threats or adjust to evolving attack patterns [37]. Consequently, researchers have employed AI and ML methodologies to improve the precision and efficacy of IDR systems. Anomaly detection, a common AI-driven intrusion detection method, recognises deviations from a system's normative behaviour as possible security risks [38]. By analysing system logs, network traffic, or user activity, it

identifies anomalous patterns that may indicate an intrusion or assault. The strategy may be implemented via several ways, including statistical analysis, distance measures, and density-based algorithms, providing a comprehensive approach to detecting anomalies and safeguarding systems [39]. Another prevalent AI intrusion detection method is supervised learning, which involves training ML models on labelled data to identify trends and forecast future results. In the context of IDR, supervised learning algorithms may be applied to discover patterns in network traffic or system logs that imply a potential attack [38].

8.3.2 Threat Intelligence

Threat intelligence is the collection, analysis, and dissemination of information on future or existing cyber threats [40]. It is essential for equipping organisations with the information necessary to safeguard against cyber threats. AI and ML techniques have been employed to augment the functionalities of threat intelligence systems, facilitating the automatic collection, analysis, and dissemination of substantial data volumes. AI and ML are extensively utilised in threat intelligence, particularly in threat hunting [41]. Threat hunting is a proactive strategy for detecting indicators of compromise and hostile activity within an organization's network infrastructure. Systems based on AI and ML considerably enhance these efforts by employing an assortment of advanced methodologies [42]. These include Natural Language Processing (NLP) for textual data analysis, deep learning techniques for pattern detection in complicated data structures, and graph analysis for mapping intricate interactions among multiple network components [43]. Employing these techniques, AI and ML-driven threat hunting platforms may independently analyse vast datasets, identify complex patterns, and detect possible threats with a degree of efficiency and precision that would be difficult to attain manually. A significant use of AI and ML in threat intelligence is in threat prediction. Threat prediction systems utilise AI and ML methodologies to examine historical data and identify patterns that may signify potential future threats. This enables organisations to implement proactive strategies to protect themselves prior to an attack [44].

8.3.3 Anomaly Detection

Anomaly detection involves identifying patterns or behaviours that deviate from the normal or anticipated behaviour of a system. It serves a vital function in cybersecurity by identifying possible security threats. AI and ML methodologies have been employed to augment the efficacy of anomaly detection systems, facilitating the identification of novel threats and adaptation to evolving assault patterns [45]. Unsupervised ML is a widely utilised AI approach for anomaly identification. Unsupervised ML algorithms utilise techniques such clustering, dimensionality reduction, and density estimation to detect patterns or behaviours that diverge from the normal or expected behaviour of a system [46].

Deep learning is another popular AI methodology for anomaly identification. Deep learning methods, including autoencoders and variational autoencoders, have been employed to detect patterns or behaviours that diverge from the regular or anticipated behaviour of a system. They do this by acquiring a low-dimensional representation of the data. Moreover, ML and AI may be utilised to improve the interpretability and explainability of anomaly detection systems. This entails employing methods such as feature selection, feature extraction, and visualisation to discern the most pertinent elements of the data and comprehend the decision-making process of the anomaly detection system [47].

The AI-ML tools integrated into HORSE offer a secure system orchestration platform that addresses the complexity of Beyond 5G (B5G) and 6G networks, particularly the challenges

posed by massive connectivity and increased attack surfaces. These tools enable vulnerability prediction, automated threat response, and threat/anomaly detection, making them highly aligned with the emerging trend of AI-driven cybersecurity solutions.

8.3.4 Digital Twins

The digital twin (DT) is the most sophisticated technology in Industry 4.0. DT technologies make it possible to create a virtual copy of the existing system and test, examine and enhance the activities, interactions, and effects of various decisions made in real-world settings. DTs provide substantial benefits in cybersecurity, providing security teams with essential tools to address complex threats and reduce risks linked to CPS in manufacturing, the IoT, and smart consumer products. DTs can be utilised in three promising sectors of cybersecurity, showcasing their prospective capabilities [48]. DTs enhance the identification of abnormal behaviour, and their significance is in facilitating swift detection and response to successfully prevent assaults. As a relatively new yet fast expanding technology, DTs provide a state-of-the-art solution to minimise a broad spectrum of hazards, correctly imitating real and virtual components, including hardware, software, and firmware systems. This capability enables real-time monitoring, comprehensive analysis, and accurate simulation of situations, hence permitting proactive cybersecurity actions and more [49].

The Network Digital Twins (NDTs) in HORSE align seamlessly with the trend of virtualization and predictive cybersecurity in 5G/6G networks. By providing virtual replicas of network infrastructures, NDTs allow operators to continuously monitor and simulate attack scenarios, enabling pre-emptive threat detection and impact analysis without risking real systems. Also, specialised NDTs enhance 5G/6G networks by embedding intelligence and automation to predict and prevent known and unknown threats. They fit market needs by reducing detection and mitigation times and generating synthetic data for training AI/ML algorithms.

8.4 Horse market adoption prospects

According to [8], the current 5G security sector is comprised by a number of manufacturers, service providers, system integrators, platform providers, and end users aiming to deliver 5G security solutions for large-scale advanced network installations. Network Services are necessary for the 5G security sector to function and end users are becoming more demanding when it comes to these services as technology trends shift. The management of a 5G security network to safeguard those services is crucial and it is new requirement for many telecom operators and corporate clients.

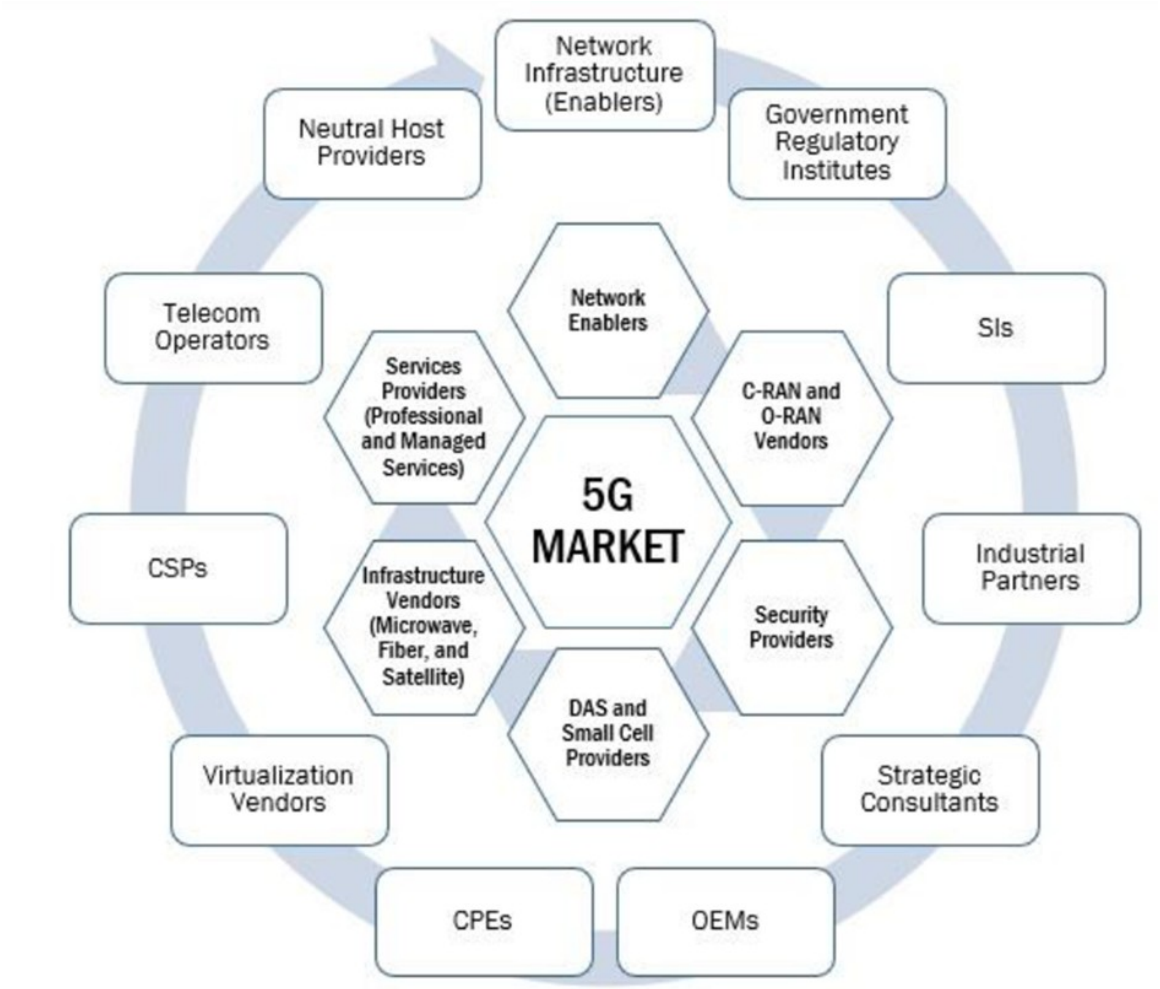


Figure 20: 5G Cybersecurity Ecosystem

Thus, the rising importance of robust cybersecurity measures in the B5G and 6G era sets the stage for HORSE's significant market impact. With an intelligent, AI-driven framework addressing both legacy and emerging security challenges, the platform aligns seamlessly with the needs of its future stakeholders (industries, governments, service providers etc.).

The advancement of 5G/6G networks envisions unparalleled capabilities in terms of connectivity, speed, and reliability. However, these advancements bring forth a dual challenge: the continuation of traditional cybersecurity threats such as DDoS attacks and the emergence of vulnerabilities unique to novel 5G/6G architectural features. In this context, the HORSE platform stands out as a promising solution specifically designed to meet these evolving requirements. Notably, it harnesses a wealth of AI, integrating modern technologies into a cohesive architecture. This architecture encompasses various concurrent ML algorithms, specialized DTs, intent-based recommendation systems, and automated mitigation systems.

In conclusion, the transition to 6G is not merely about amplifying existing capabilities but is a holistic transformation poised to redefine the landscape of mobile communication. As research continues to explore innovative architectures and security frameworks, the impending era of 6G promises to deliver advanced functionalities, enhanced intelligence, and fortified security—all of which are essential for addressing the challenges of an increasingly connected world.

9 Preliminary SWOT Analysis

Figure 21: HORSE SWOT Schema

9.1 Strengths

9.1.1 Threat Detection (DEME) with Machine Learning Algorithms

One of the major strengths of the HORSE platform lies in the use of sophisticated machine ML algorithms for threat detection and high-level mitigation advice. The Detector and Mitigation Engine (DEME) will operate in the “real context”, meaning it will be able to provide real time protection to the real infrastructure. With the help of DEME, HORSE can better identify threats targeting the 5G/6G infrastructure by utilizing the combined intelligence of several ML models. The system can quickly identify and classify potential security risks, including virus and intrusion attempts, as well as unusual behaviour suggestive of insider threats, by continually analysing network traffic patterns, anomalies, and known threat indicators. We need to lay emphasis on the fact that the DEME is completely ML oriented, meaning that the module can recognize when the behaviour of the network is normal and detect any unnatural behaviour patterns that could indicate an attack is happening. Such an approach that deviates from the traditional signature based or hybrid threat detection systems still in use today, elevates HORSE’s capabilities in the threat detection field.

9.1.2 Network Digital Twin

Apart from the “real context” HORSE also utilizes an “emulated context” in parallel. This “emulated context”, which is a virtual image of the 5G/6G network, is made possible with Network Digital Twin (NDT) technology. Real-time monitoring and analysis of network performance, traffic patterns, and safety measures are made possible by this “network in network” approach. This way a sandbox environment is created, ideal for experimentation.

This experimentation includes prediction of possible attack pathways, proactive identification of vulnerabilities, and evaluation on the effect of security events by simulating different network settings and configurations. This sandbox environment consists of two digital twin components, each one dedicated to a specific purpose.

9.1.2.1 Network Digital Twin Predictive Network Maintenance

Through constant observation and examination of the emulated environment the Detection & Prediction DT is tasked with predicting anomalies and threats based on network's performance metrics and health indicators. The DT then suggests mitigation actions and preventive strategies, which combined with the results from the “real context” offer insight on the present and future state of the monitored 5G/6G network. More specifically, this service offers automated construction functionalities, detecting network topology, traffic flows, and services, or allows for offline construction through predefined configurations. Leveraging advanced network emulation technologies, HORSE’s DT replicates a complete 5G network on a single device. Developed collaboratively, it extends existing emulation capabilities, enabling easier application deployment and supporting the evolution towards 6G networks. During execution, the DT maintains real-time synchronization with the actual network, providing predictive analytics and alerts to support decision-making. By continuously analysing network data, it identifies anomalies and potential security threats, allowing for proactive mitigation actions. This innovative approach revolutionizes network management by providing a virtual sandbox environment for testing and optimizing network configurations, ultimately enhancing network reliability, security, and performance.

9.1.2.2 Network Digital Twin Impact Analysis

The Impact Analysis Digital Twin is poised to revolutionize the monitoring capabilities of HORSE modules through emulation. By initially employing synthetic data and following a cloud-native approach, this DT encompasses all network elements, not just those within the HORSE project, allowing seamless integration with real equipment. For instance, it can emulate gNodeBs or operate alongside genuine hardware within the same environment. The development of this DT includes novel features such as transport connectivity, advanced telemetry collection, ML models, and automated network topology and attack pattern definition. This innovative approach transforms impact analysis by offering a comprehensive ecosystem for monitoring and analysing network behaviour, enhancing adaptability, scalability, and efficiency in network management.

9.1.2.3 Network Digital Twins in the cybersecurity field

Through the process of building a virtual network architecture, which includes devices, apps, and communication protocols, the system can replicate penetration testing scenarios, security policy modifications, and cyberattacks in a controlled environment. This helps security professionals to find potential weaknesses and attack routes, verify security configurations, and evaluate how effective current security controls are. In addition, security staff can use the Network Digital Twin as a training platform where they can practice responding to simulated cyber threats and incidents.

9.1.2.4 Intent Based Security Operations

In today's rapidly evolving technological landscape, the demand for efficient and adaptable network management solutions has become increasingly paramount. Intent based security operations are another selling point of HORSE, with the Intent Based Interface (IBI) module as its cornerstone. In general, IBI strives to streamline network configuration and operation by receiving high-level directives from network managers or software agents. IBI is then responsible for aligning the received high-level intents with the configured policies, and mapping these intents into security workflows. These security workflows are able to react to threats and vulnerabilities. In conclusion, the adoption of intent-based operations, as exemplified by the IBI module in HORSE, is instrumental in addressing the evolving challenges and complexities of modern network management. By streamlining configuration, automating tasks, enhancing security, and simplifying management, intent-based operations empower organizations to unlock new levels of efficiency, agility, and resilience in today's dynamic digital landscape.

9.1.3 Security Management Automation

The above modules are the most prevalent among HORSE's automation features, helping to create a fully automated workflow. From the detection of an attack all the way to the enforcement of mitigation policies, HORSE automates a plethora of security operations. Automated workflows reduce the effect of security breaches on the targeted network by enabling quick incident response, threat mitigation, and policy enforcement. Automation also improves scalability and agility, making it possible for the system to effectively handle security in diverse and remote network environments. We have to emphasize that, while we have seen significant effort in automating threat and anomaly detection, the mitigation part for an attack always required human intervention. In HORSE we aim towards a more hybrid approach, where the system itself is able to propose mitigation advices, translate them to applicable policies and rules and finally enforce them where needed.

9.2 Weaknesses

9.2.1 Low TRL

One of HORSE’s main weaknesses is the system's overall low TRL, which implies some implementation and deployment immaturity. On many occasions this could be the result of issues like low R&D, insufficient real-world testing, or a lack of broad adoption in operational situations. Consequently, the system may have difficulties with dependability, expandability, and compatibility, which could impede its efficiency in actual real-world scenarios. If we examine the current state of HORSE, we can observe that the average TRL amongst the architectural components will be reaching a 4 or a 5. These numbers of course do not allow HORSE to enter the market and antagonize other solutions currently in use, but we also need to emphasize that lower TRLs are common in such projects. Having said this, our consortium is determined to improve and develop each component to a decent TRL by the end of the project. This means that HORSE’s outcomes could be exploited in future projects, individual products and even foster partnerships between the consortium’s organizations.

9.2.2 Limitations in addressing threats dedicated to the 5G/6G plane

Although the system has sophisticated threat detection capabilities, it is not always able to defend against threats which especially target the unique design and features of the 5G/6G network. The attacks currently tested against the network topology guarded by HORSE are DDoS and DoS attacks. These are well known threats by now and have been used extensively to overwhelm a huge number of networks and infrastructure. One might argue that these attacks do not demonstrate HORSE's capabilities in the current 5G and future 6G world. In the second iteration of the project, the consortium's goal is to integrate more advanced and sophisticated threats targeting 5G core vulnerabilities. It would be neglectful to omit attacks like DDoS though, just because they do not exploit a vulnerability dedicated to 5G. Every 5G topology still relies on some basic components found everywhere, e.g. DNS or NTP servers. These parts have been a standard target for DDoS attempts and still need to be protected to ensure the seamless and uninterrupted operation of any network infrastructure.

9.2.3 Mitigation action database

The lack of an extensive Mitigation Action Database is another weakness in the system that may make it harder for it to react effectively and inside a reasonable time frame in the face of new threats. At the current state of the project the need for a pre-established mitigation action repository has become apparent. Having such a tool in our arsenal, could determine how efficiently we can protect a system and replenish from an attack that already managed to cause harm. The implementation of an initial Mitigation Action Database has already started, with some initial mitigation actions already occupying it. We need to note here that this is still a prototype and includes only straightforward and simple actions. In order to confidently claim that we have a complete mitigation rule enforcement workflow, our knowledge base needs to be occupied with actions, rules and terminology dedicated to the HORSE project.

9.3 Opportunities

9.3.1 Expanding 5G/6G Market

The Horse system will gain a great deal from the 5G and 6G markets' ongoing growth and expansion. Strong cybersecurity solutions designed for these cutting-edge networks are in greater demand as 5G and 6G technology spreads throughout numerous industries and sectors. Sectors such as industrial networks relying on 5G/6G services as well as private networks could benefit immensely from security solutions like HORSE. HORSE has the chance to take advantage of this growing uptake of 5G and 6G technologies and position itself as a top supplier of cybersecurity solutions for next-generation networks. In the growing 5G/6G ecosystem, HORSE can secure its competitiveness and penetrate new markets by establishing itself as a reliable partner in protecting connected devices, sensitive data, and critical infrastructure.

9.3.2 Integration of 5G/6G in Diverse Environments

The integration of 5G/6G technology across various environments, such as industrial applications, IoT ecosystems, smart cities, and autonomous vehicles, presents another

opportunity for the system. Cybersecurity solutions that can handle the unique security problems presented by such environments are becoming more and more necessary as 5G/6G networks become essential to enabling advanced use cases and digital transformation projects in these sectors. HORSE solution can increase its market reach and relevance while meeting the changing needs of many stakeholders and consumers by customizing its capabilities to match the particular security requirements and use cases of various industries and applications. This gives the system a chance to work with industry leaders, form strategic alliances, and promote innovation in cybersecurity solutions for developing 5G and 6G-enabled environments.

9.3.3 Rising Demand for Advanced Threat Detection and Prevention

Advanced threat detection and prevention capabilities are in high demand due to the increase in sophisticated cyber threats targeting 5G and 6G networks. HORSE is well-positioned to meet this need because of its strengths in intent-based security operations, network digital twin technologies, and ML algorithms for threat identification. Through continuous innovation and improvement of its detection and mitigation capabilities against developing cyber threats, the system can take advantage of the expanding market for cybersecurity solutions customized to the particular difficulties of 5G/6G networks. This offers the system a chance to stand out from the competition, draw in new clients, and position itself as a reliable authority on 5G and 6G cybersecurity.

9.4 Threats

9.4.1 Competition from Established Players

The presence of multiple well-established entities in the sector, including cybersecurity firms and Mobile Network Operators, poses a significant threat to the system. Because of their vast resources, market power, and existing customer base, these industry leaders provide formidable obstacles to entry for new players, such as HORSE. The presence of these well-established competitors could lead to problems including pricing pressure, market saturation, and difficulty acquiring market share or forming strategic alliances. Furthermore, to offer competitive cybersecurity solutions, established firms may take advantage of their current infrastructure and customer base. This would increase competition and may restrict the system's market reach and growth prospects.

9.4.2 Emergence of Advanced Cyber Attacks Targeting 5G/6G Networks.

Emergence of new and sophisticated cyberattacks designed to target vulnerabilities in 5G/6G networks poses a serious danger to any new security solutions like HORSE. Adversarial parties always turn their attention to recently adopted and widely used technologies, attempting to identify exploitable vulnerabilities. Recent history is filled with such examples where state of the art security measures have failed because of a zero-day exploit. It would be naive to assume that current 5G and future 6G will be without design flaws or impenetrable. Potential weaknesses in software-defined infrastructure, network protocols, or cutting-edge technologies like edge computing and network slicing could be exploited by these assaults, putting network availability, data privacy, and integrity at serious danger. In conclusion, such new and unidentified attacks could potentially render systems like HORSE obsolete.

9.4.3 Regulatory and Compliance Challenges

Threats from regulatory and compliance problems may also affect the Horse system; this can be relevant for highly regulated sectors like cybersecurity and telecommunications. Ensuring compliance with evolving standards relating to data privacy, cybersecurity, and network resilience may provide issues for the system as governmental and regulatory agencies impose stronger restrictions and requirements. Failure to adhere to regulatory rules may lead to legal consequences, monetary fines, and loss of trust among clients.

9.4.4 Limited Adoption Potential

The lack of clear commercialisation pathways, the presence of competing technologies, the lack of engagement with key stakeholders, and limited alignment with changing market demands are some of the factors that may make it difficult for the HORSE outcomes to be widely adopted. All of these barriers could hinder the efficient dissemination and use of the project's outcomes, thus diminishing its overall impact, scalability, and market reach. Collaboration with industry leaders and standardisation bodies such as 3GPP or IEEE, as well as engagement with credible market research, guarantees that the project technologies have the capacity to satisfy emerging standards and interoperability requirements. Moreover, establishing strategic alliances with early adopters in the telecommunications and cybersecurity industries helps authenticate the project's solutions and facilitate broader acceptance. The risk of limited utilisation is minimal, as the project's technologies are essential for the future development of secure and intelligent digital infrastructures, as indicated by the market analysis.

9.5 Summary

The implementation of the Horse system is expected to result in significant results in the field of cybersecurity, specifically in protecting 5G and 6G networks from constantly changing threats. By utilizing ML algorithms and NDT technology, the system's superior threat detection capabilities enable it to proactively identify and mitigate possible cyber threats, hence improving network resilience and integrity. Its compatibility with intent-based security operations also makes it possible to implement strategic reaction plans that are customized to company goals, guaranteeing a flexible and unified security posture. The Horse system may take advantage of the opportunity provided by the growing 5G/6G market and a variety of integration scenarios, even in the face of obstacles like low TRL and competition from established providers, to position itself as a leader in next-generation cybersecurity. In the era of 5G and 6G technology, addressing regulatory compliance and future threats is still crucial. To fully meet the system's potential in protecting critical infrastructure and advancing cybersecurity, ongoing innovation, investment, and collaboration are required.

10 Preliminary PESTLE Analysis

Since HORSE is a 5G/6G project, touching a variety of technologies, each technology with each own particularities, it is crucial to demonstrate how external factors could potentially affect the project. These factors can be categorized as Political, Economic, Social, Technological, Legal and Environmental (PESTLE). By conducting this analysis, we aim to demonstrate how these external factors can potentially affect the project's course, as well as understand the intricacies of each field. Figure 22: HORSE PESTLE Analysis summarizes the contents of HORSE's PESTLE analysis.

Figure 22: HORSE PESTLE Analysis

10.1 Political Analysis

Government Regulations and Policies: An increasing focus on data privacy, national security, and protecting key infrastructure characterizes the political environment around cybersecurity and telecommunications. Around the world, governments have introduced laws and regulations to improve cybersecurity and protect against cyberattacks, especially in relation to 5G and 6G networks. The EU has greatly improved cybersecurity by adopting laws like the General Data Protection Regulation (GDPR) and the Network and Information Security Directive. These regulations aim to improve data security and establish a standard for cybersecurity obligations among participating countries. The EU's emphasis on privacy and security has influenced the evolution of the European cybersecurity sector, causing enterprises to modify their offerings in order to comply with legal regulations.

Government Funding and Support: Opportunities for the system's development and implementation are provided by government funding programs and assistance for cybersecurity activities. Working together with governmental organizations, academic institutions, and business consortiums can open doors to capital, resources, and know-how which will promote innovation and improve the system's performance. The system can position itself to take advantage of government assistance and help achieve national cybersecurity goals by positioning itself in line with government priorities for infrastructure protection, technology development, and cybersecurity research.

Collaboration across national borders: Cyber threats are transnational, demanding cooperation among European nations. The European Union has been trying to create a coordinated cybersecurity policy that promotes information sharing and cooperative response systems. To develop cutting-edge cybersecurity solutions, initiatives like the European Cybersecurity Industrial, Technology, and Research Competence Centre aim to promote cooperation between member states, the academic community, and industry. Standardizing security certification throughout the Union is another goal of the establishment of the EU Cybersecurity Certification Framework.

Public-private partnerships: European governments understand how important it is to involve businesses in solving cybersecurity challenges. Creating public-private partnerships has grown to be a crucial aspect of the cybersecurity market in Europe. Governments collaborate with industry players to develop cybersecurity plans, share threat intelligence, and encourage investment in research and development. These partnerships not only close the knowledge gap but also foster innovation and the exchange of best practices.

International Relations and Geopolitical Factors: International relations and geopolitical tensions may have an impact on the system's market dynamics and regulatory framework. Market access, supply chain integrity, and regulatory harmonization initiatives can be impacted by trade conflicts, diplomatic difficulties, and security concerns between nations. Furthermore, geopolitical factors could influence government regulations against foreign participation in cybersecurity and critical infrastructure projects, which could have an impact on the system's international collaborations and growth.

Cybersecurity skills gap: The scarcity of cybersecurity professionals is a global problem, especially in Europe. A political attempt has been made to close the skills gap by implementing training and educational initiatives. Governments collaborate with academic institutions and business leaders to provide specialized programs and to promote cybersecurity as a career option. In order to guarantee that the market has a consistent supply of knowledge, the EU's Digital Skills and Jobs Coalition aims to close both the cybersecurity workforce gap and the digital skills gap.

Summary: The European cybersecurity sector is defined by a combination of factors such as regulatory frameworks and support by governments, international cooperation, public-private partnerships, geopolitical considerations and efforts to address the skills gap. As Europe continues to deal with rising cyberthreats, political actions and strategic measures will be crucial to sustaining a robust and resilient cybersecurity ecosystem. Opportunities have arisen for the HORSE solution's deployment because our product conforms with rules. All things considered, the political environment in the EU is conducive to the launch of our product.

10.2 Economic Analysis

Industry size and expansion: The market for 5G security is projected to increase at a compound annual growth rate of 38.8% between 2023 and 2028, from USD 1.7 billion in 2023 to USD 9.2 billion by 2028 [15]. The sector is expanding due to the increasing sophistication, targeting, and complexity of defending against cyberattacks. Businesses need to invest in increasingly robust security measures as cyberattacks become more sophisticated in order to stay safe. This means educating staff members on appropriate security procedures and making investments in cutting-edge security technology like machine ML and AI.

Cost of Development and Deployment: Significant initial costs for talent acquisition, technical infrastructure, and research and development are associated with the system's development and implementation. To provide a reliable and competitive solution, investment in state-of-the-art technologies is required, such as cybersecurity automation tools, machine learning algorithms, and network digital twin technology. Costs related to system integration, deployment, and modification for particular client needs also need to be taken into account.

Competitive environment: Intense competition and active engagement from both domestic and foreign suppliers define the European cybersecurity market. International cybersecurity titans like Symantec (now a part of Broadcom), Cisco Systems, IBM Security, and Trend Micro are a few of the well-known significant firms in this sector. Notable local firms in the sector are also Kaspersky Lab (Russia), F-Secure (Finland), Sophos (UK), and CyberArk (Israel), all of whom have made significant advances. Furthermore, the European cybersecurity environment supports a thriving ecosystem of newcomers and creative solution providers, which boosts the industry's technological innovation and competitiveness.

Opportunities and Challenges: The European cybersecurity sector has a lot of room to grow, but it also faces a lot of obstacles. The biggest of them is a serious lack of skilled cybersecurity staff, requiring immediate steps to close the gap through activities in education, training and finally more automated security solutions. The dynamic threat landscape, which includes ransomware, social engineering techniques, and sophisticated malware, need constant innovation and adaptability in cybersecurity solutions. Furthermore, cybersecurity companies have challenges as well as possibilities in adhering to data protection rules such as GDPR. Establishing alliances and encouraging cooperation amongst various stakeholders, such as businesses, governmental organizations, and cybersecurity vendors, is essential to addressing these problems and promoting a more secure ecosystem. In summary, despite its persisting challenges, the European cybersecurity sector holds great promise.

HORSE maturity: The potential difficulty in scaling project outcomes beyond research and innovation (R&I) frameworks poses a significant financial risk for adopters within every sector. Since many companies, organizations and partners are often resistant to

modifications in their core functions, early adopters might face prolonged integration periods, delaying the realization of benefits such as increased efficiency or cost savings. This delay can lead to higher operational costs as companies continue to rely on less efficient legacy systems. Furthermore, the initial investments made in adopting the new technology might not yield the expected returns in the short term, affecting the financial stability and planning of these organizations. Adopters may also incur additional costs related to regulatory compliance and system compatibility, further straining their budgets. Overall, the financial impact includes not only delayed returns on investment but also potential increased costs and economic uncertainty.

Summary: The overall condition of the economy is favourable to the development of new products. More specifically, because HORSE paradigms are compatible with the future operation of the European cybersecurity market. HORSE only has to prove it is a mature and easy to integrate solution, making the costs for its adoption worthwhile.

10.3 Social Analysis

Cybersecurity Awareness and Education: The social environment around cybersecurity is defined by people, organizations, and governments being more conscious of and concerned about data privacy issues and cyberthreats. Strong cybersecurity procedures are becoming increasingly important to safeguard sensitive data, vital infrastructure, and personal information as cybersecurity breaches become more frequent and significant. Furthermore, funding cybersecurity education and awareness initiatives can support the development of resilience and cybersecurity knowledge in society as well as increase public awareness and trust.

Privacy and Data Protection: Specifically, the GDPR has significantly impacted the European cybersecurity industry. Because of GDPR, which has raised spending on cybersecurity solutions, organizations are placing a higher priority on data protection. Demand for robust cybersecurity measures is rising as citizens of Europe, who are increasingly conscious of their rights and privacy, expect companies to manage their data responsibly.

Digital Inclusion and Accessibility: In order to advance digital inclusion and socioeconomic development, access to cybersecurity solutions and digital technology is crucial. It is important for the system to aim for accessibility and inclusivity for people from different socioeconomic origins, abilities, and backgrounds. We already see this happening with the 5G infrastructure expanding rapidly in urban centres. This could entail creating interfaces that are easy to use, supporting multiple languages, and making sure that a variety of devices and network environments are compatible.

Industry-specific issues: Industry-specific problems affect the cybersecurity environment worldwide. Telecommunication providers must consistently protect their infrastructure, as the population increasingly relies on it for various critical services. Other examples include the banking sector, which deals with cybercrime and financial fraud, the healthcare industry, which needs to protect patient data, and important infrastructure sectors, like transportation and energy, which are at risk from operational system failure. Industry-specific legislative restrictions and certain sociocultural conditions impact the need for and acceptability of cybersecurity solutions.

Trust and Collaboration: Collaboration and trust are essential to the system's success as well as the efficacy of cybersecurity initiatives. Fostering adoption, engagement, and long-term relationships among stakeholders—including consumers, partners, regulators, and the

general public—requires developing trust. Transparency, honesty, and accountability ought to be given top priority by the system in all of its dealings with stakeholders and in communications. Moreover, boosting collaboration and the sharing of knowledge across stakeholders—including government organizations, telecommunication providers, cybersecurity communities, and partners in the industry—can improve overall resilience and reaction capacities against cyberthreats.

Summary: To create effective tactics, foster adoption, and ensure a secure digital environment, politicians, corporations, and cybersecurity providers ought to possess an extensive understanding of the social dynamics and sociological aspects impacting the European cybersecurity domain. The social environment can be viewed as neutral for the HORSE system for these reasons.

10.4 Technological Analysis

5G threat landscape: The threat landscape involving 5G technology's fundamental structure is complicated and raises a number of security issues. This environment includes flaws in Network Function Virtualization and Software-Defined Networking which allow for network flexibility but can be used by hackers. One essential element of 5G networks is edge computing, which necessitates strict security measures to prevent unauthorized access. One of the challenges that comes with implementing network slicing is protecting several virtual networks which are running on the same physical infrastructure. The security matrix is further complicated by possible interoperability problems, device authentication and encryption flaws, and firmware and software vulnerabilities within network devices. Furthermore, persistent threats to 5G network integrity include hardware vulnerabilities, zero-day exploits, and open-source software management. These require continuous awareness and proactive mitigation efforts.

Emerging Technologies and Innovations: Cybersecurity requires AI and ML to be effective. These technologies enable the development of advanced analytics and detection systems with immediate detection capabilities of patterns, anomalies, and prospective threats. AI and ML algorithms enhance the efficacy of security operations and incident response by facilitating faster and more accurate threat detection and response. In addition, hackers now have a larger attack surface due to the proliferation of connected devices and the IoT. Data security, networks, and IoT devices face serious security issues. European cybersecurity solutions heavily emphasize the integration of strong authentication, encryption, and access control approaches to ensure the security and privacy of IoT deployments.

Cloud security: As cloud computing services are being used more often, new security risks have surfaced. With more European businesses utilizing cloud-based platforms, apps, and infrastructure, robust cloud security solutions are needed. Cloud security solutions, such as secure cloud gateways, cloud workload protection platforms, and cloud access security brokers, safeguard data and applications in cloud environments.

Security automation and orchestration: The increasing frequency and complexity of cyber-attacks necessitates the use of security automation and orchestration solutions to improve incident response and reduce reaction times. European cybersecurity solutions combine security tools, expedite security operations, and accelerate threat detection, analysis, and remediation through automation and orchestration.

Summary: The European cybersecurity market is driven by the ongoing technological development needed to defend against emerging attacks, protect sensitive data, and

safeguard digital infrastructure. By comprehending these technological developments, businesses and cybersecurity service providers can stay ahead of the ever-evolving threat landscape and offer efficient cybersecurity solutions. The technological environment in the EU is thought to be conducive for the introduction of our product.

10.5 Legal Analysis

General Data Protection policy (GDPR): The GDPR is a significant data protection law that came into force in 2018 and has a major impact on the cybersecurity market in Europe. It outlines obligations for companies handling personal data as well as legal requirements for data protection. The GDPR requires organizations to ensure data processing is transparent, notice data breaches, and put in place the appropriate security measures to protect personal data.

Intellectual Property Protection: Protecting the system's developments, technologies, and proprietary assets requires intellectual property protection. Securing patents, trademarks, and copyrights for crucial technologies, algorithms, and software elements offers defence against unauthorized utilization, duplication, and violations by rivals. Furthermore, putting strong contracts, non-disclosure agreements, and license agreements in place with vendors, consumers, and partners protects the intellectual property rights of the system and guarantees just recompense for its discoveries.

Contractual and Regulatory Compliance: When deploying and operating the system, contractual and regulatory compliance requirements must be carefully taken into account. Contracts related to data protection, cybersecurity, service level agreements, and regulatory compliance may be found in agreements with clients, partners, and vendors. Maintaining compliance with regulatory requirements and contractual responsibilities reduces the likelihood of legal issues, contract violations, and reputational damage.

National Cybersecurity Laws: In addition to EU-wide restrictions, every EU member state has its own national cybersecurity laws and regulations. These guidelines may include specific requirements for managing problems, protecting critical infrastructure, reporting security breaches, and exchanging data. The UK's Cybersecurity and Data Protection Act and Germany's IT Security Act are two examples.

Regulatory agencies: In each of their home countries, national data protection agencies play a crucial role in maintaining cybersecurity and data protection legislation. These DPAs are able to investigate data breaches, impose fines for noncompliance, and provide guidance on cybersecurity best practices.

Summary: It is critical for companies operating in the European cybersecurity sector to understand the regulatory landscape and compliance requirements. Adhering to these regulations not only saves companies money on fines but also enhances consumer and corporate confidence, transparency, and data security throughout Europe. To sum up, HORSE solutions offer GDPR-compliant technologies that respect privacy and security. Because of this, the legal environment is thought to be favourable for the HORSE project's start.

10.6 Environmental Analysis

Data centers, network infrastructure, and security systems: All require a significant energy expenditure for cybersecurity operations. As the European cybersecurity industry

grows, energy consumption needs to be assessed and optimized in order to minimize the impact on the environment. Adopting sustainable data centre practices, renewable energy sources, and energy-efficient technologies can all help reduce carbon footprints.

Energy Consumption and Environmental Impact: The rapid advancement of technology and the continuous improvement of cybersecurity protocols are major factors in the generation of electronic waste. One of the laws and regulations addressing e-waste management in European nations is the Waste Electrical and Electronic Equipment Directive. It is critical to adhere to ethical recycling and disposal practices for old or end-of-life cybersecurity equipment in order to minimize the impact on the environment.

Green initiatives and sustainability: Companies are adopting green initiatives and sustainable business practices more rapidly, particularly those in the cybersecurity sector. This means using renewable energy sources, implementing eco-friendly policies, and integrating sustainability issues into their day-to-day operations. Environmentally conscious certifications and standards such as ISO 14001 reflect an organization's commitment to environmental responsibility.

Environmental directives and rules: Environmental policies and regulations, including the EU's Green Deal and its initiatives to promote a circular economy, may have an influence on the methods and tactics used by cybersecurity companies. Maintaining environmental regulations and aligning cybersecurity efforts with sustainability goals can boost a business's standing and competitiveness in the marketplace.

Consumer demand and awareness: Concerns about the environmental impact of the products and services they use are growing among European consumers. By exceeding customer expectations and attracting environmentally conscious clients, cybersecurity service providers who can demonstrate their commitment to sustainability and environmental responsibility may gain a competitive advantage.

Summary: It is essential to consider the environmental impact of the European cybersecurity business in order to encourage sustainable practices, reduce carbon emissions, and align with the broader goals of environmental protection and sustainability. Adopting sustainable practices, optimizing energy efficiency, and embracing green technologies could lead to an industry that is more ecologically sensitive. Because of this, the legal environment is favourable for the HORSE project's start.

11 HORSE Contributions to EU Sustainable Development Goals as part of the UN 2030 Agenda for Sustainable Development

The United Nations' 2030 Agenda for Sustainable Development [20] outlines a comprehensive blueprint aimed at achieving a better and more sustainable future for all. Central to this agenda are the 17 Sustainable Development Goals (SDGs), which address global challenges such as poverty, inequality, climate change, environmental degradation, peace, and justice. These goals are designed to accomplish several key objectives:

- **Eradicate Poverty (Goal 1):** This goal aims to end poverty in all its forms everywhere, ensuring that all people, particularly the most vulnerable, have equal rights to economic resources and basic services.
- **Zero Hunger (Goal 2):** It seeks to end hunger, achieve food security, improve nutrition, and promote sustainable agriculture by ensuring access to sufficient and nutritious food for all people.
- **Good Health and Well-being (Goal 3):** This goal focuses on ensuring healthy lives and promoting well-being for all at all ages by reducing maternal mortality, ending epidemics of communicable diseases, and achieving universal health coverage.
- **Quality Education (Goal 4):** It aims to ensure inclusive and equitable quality education and promote lifelong learning opportunities for all, emphasizing the importance of early childhood development, primary and secondary education, and skills for employment.
- **Gender Equality (Goal 5):** This goal strives to achieve gender equality and empower all women and girls, by eliminating all forms of discrimination and violence against women and girls and ensuring their full participation in leadership and decision-making processes.
- **Clean Water and Sanitation (Goal 6):** Ensuring availability and sustainable management of water and sanitation for all is the focus here, aiming to provide safe and affordable drinking water, adequate sanitation, and hygiene for all, while also addressing water scarcity.
- **Affordable and Clean Energy (Goal 7):** This goal seeks to ensure access to affordable, reliable, sustainable, and modern energy for all, promoting renewable energy sources and improving energy efficiency.
- **Decent Work and Economic Growth (Goal 8):** It aims to promote sustained, inclusive, and sustainable economic growth, full and productive employment, and decent work for all, focusing on higher productivity and technological innovation.
- **Industry, Innovation, and Infrastructure (Goal 9):** This goal focuses on building resilient infrastructure, promoting inclusive and sustainable industrialization, and fostering innovation, aiming to develop quality, reliable, sustainable, and resilient infrastructure to support economic development and human well-being.
- **Reduced Inequalities (Goal 10):** It aims to reduce inequality within and among countries by empowering and promoting the social, economic, and political inclusion of all, irrespective of age, sex, disability, race, ethnicity, origin, religion, or economic or other status.

- **Sustainable Cities and Communities (Goal 11):** This goal seeks to make cities and human settlements inclusive, safe, resilient, and sustainable by ensuring access to adequate, safe, and affordable housing and basic services, and upgrading slums.
- **Responsible Consumption and Production (Goal 12):** It aims to ensure sustainable consumption and production patterns, promoting resource and energy efficiency, sustainable infrastructure, and providing access to basic services, green jobs, and a better quality of life for all.
- **Climate Action (Goal 13):** This goal calls for urgent action to combat climate change and its impacts, by strengthening resilience and adaptive capacity to climate-related hazards and natural disasters in all countries.
- **Life Below Water (Goal 14):** It focuses on conserving and sustainably using the oceans, seas, and marine resources for sustainable development, addressing marine pollution, ocean acidification, and overfishing.
- **Life on Land (Goal 15):** This goal aims to protect, restore, and promote sustainable use of terrestrial ecosystems, manage forests sustainably, combat desertification, halt and reverse land degradation, and halt biodiversity loss.
- **Peace, Justice, and Strong Institutions (Goal 16):** It seeks to promote peaceful and inclusive societies for sustainable development, provide access to justice for all, and build effective, accountable, and inclusive institutions at all levels.
- **Partnerships for the Goals (Goal 17):** This goal emphasizes strengthening the means of implementation and revitalizing the global partnership for sustainable development, encouraging and promoting effective public, public-private, and civil society partnerships.

These goals are interlinked and are designed to leave no one behind, creating a framework for sustainable development that balances economic, social, and environmental dimensions. Regarding the HORSE paradigm it is apparent that it does not fit under all of UN's goals, as they cover a plethora of issues around the world. The two goals that align with the philosophy of our project are 9 and 11, due to HORSE's holistic, omnipresent and resilient characteristics that safeguard current 5G and future 6G services and environments.

11.1 Resilient Infrastructure and Innovation

The United Nations' goal to achieve resilient infrastructure and foster a world of continuous innovation [21] aligns closely with HORSE's mission to create a secure environment for 5G and 6G services through cutting-edge cybersecurity solutions. The UN's initiative to expand mobile broadband infrastructure globally, particularly in developing regions with limited existing infrastructure, underscores the importance of projects like HORSE. These projects become increasingly vital as they provide the necessary security framework to protect the digital landscape from evolving threats. Although the UN's objectives do not explicitly highlight resilience against digital or cyber threats, such considerations are implicit in ensuring the robustness and sustainability of infrastructure. In today's interconnected world, digital and cyber threats pose significant risks to network services and the industries that depend on them. Thus, advancing and implementing comprehensive cybersecurity measures, like those offered by HORSE, is crucial for safeguarding the integrity and resilience of both current and future infrastructures.

Cybersecurity systems like HORSE are essential in creating resilient infrastructures capable of withstanding and quickly recovering from cyberattacks. These systems employ a variety of

innovative solutions to detect, prevent, and respond to cyber threats, ensuring the continuous and reliable operation of 5G and 6G networks. As these networks form the backbone of modern and future smart cities, industrial IoT applications, and global communication, their security is paramount. Projects focused on cybersecurity not only protect data and communication channels but also build trust and reliability into the technology ecosystem, fostering further innovation and adoption.

In the context of the UN's broader goal to enhance infrastructure, deploying secure and resilient broadband services can drive socio-economic development, particularly in underserved regions. The proliferation of secure mobile broadband can support education, healthcare, and economic activities by providing reliable access to information and communication technologies. As such, cybersecurity solutions like those developed by HORSE become integral to the success of these initiatives, ensuring that the benefits of modern connectivity are not compromised by vulnerabilities. Consequently, investing in robust cybersecurity frameworks is not just about protecting digital assets; it is about enabling sustainable and resilient development on a global scale.

11.2 Sustainable cities and communities

Achieving Goal 11 of the United Nations' 2030 Agenda, which aims to make cities and human settlements inclusive, safe, resilient, and sustainable [23], is closely linked with advancements in technology, particularly through the deployment of 5G, future 6G networks, and the integration of Internet of IoT devices. 5G technology offers unprecedented high-speed and low-latency connectivity, essential for real-time operation of various smart city applications. For instance, smart traffic management systems can use 5G to dynamically adjust traffic signals, reducing congestion and emissions, while smart grids can more efficiently distribute energy, thereby lowering consumption and costs. Future 6G networks are expected to further enhance these capabilities, providing even higher data rates, improved energy efficiency, and ubiquitous coverage, which will be crucial for sophisticated AI-driven urban management systems, enhanced virtual reality, and augmented reality applications that can transform urban living. The integration of IoT devices within smart city infrastructure is another pivotal element. IoT sensors embedded in buildings, roads, and public utilities can continuously monitor and manage urban infrastructure, optimizing maintenance schedules, predicting failures, and enhancing resource efficiency. Environmental monitoring systems using IoT can track air quality, manage waste, and monitor water supply, ensuring sustainable consumption and reducing pollution. Moreover, advanced IoT-enabled public services, such as smart lighting and waste management systems, can significantly improve urban living conditions by conserving energy and promoting efficient resource use. These technological advancements are fundamental in creating more resilient urban environments capable of adapting to and mitigating the impacts of climate change and natural disasters.

However, the implementation of these advanced technologies necessitates robust security measures to protect against external threats. Ensuring data security is paramount, requiring encryption of data in transit and at rest, alongside strong authentication and access control mechanisms to prevent unauthorized access. Network security must also be reinforced through advanced firewalls, intrusion detection systems , and secure network architectures that isolate critical infrastructure from less secure segments. IoT device security involves regular updates and patches to fix vulnerabilities, secure boot processes to ensure only trusted software runs, and unique device identities for robust authentication. Additionally, resilience against cyber-attacks is critical, necessitating protection against Distributed Denial of Service (DDoS) attacks, comprehensive backup and disaster recovery plans, and

continuous monitoring to detect and respond to threats in real-time. HORSE adheres to these requirements offering solutions for many of the aforementioned problems and ensuring sustainability and resiliency in modern cities. Through such innovative projects, smart cities can harness the full potential of technological advancements while ensuring the safety and security of their inhabitants.

12 Standardisation

Establishing a relevant European research and technology ecosystem focused on advancing next-generation network technologies, requires a strong commitment to standardisation, whatever the means: pre-standardisation activities, formal standards development, open-source communities, etc. Standardization not only ensures interoperability, reliability, and scalability within telecommunications but also fosters collaboration and innovation across diverse stakeholders and contributes to the consolidation of an open and sustainable technology ecosystem.

12.1 Objectives

HORSE standardisation activities have a double objective: fostering industry collaboration on open and interoperable solutions in Europe and beyond, and driving the enhancement of next-generation network security during the lifetime of the project and even beyond its end.

Through active participation and strategic collaboration, the project aims at consolidating a relevant influence on technology development and the associated policy decisions, mainly at the European level, but also considering national frameworks and a global dimension.

12.2 Standardisation Plan

To ensure that the project outcomes have maximum impact in the technology and policy aspects mentioned above, HORSE started an active supervision of relevant communities and identified the opportunities whit highest impact coming from projects results. This is a continuous activity, which will require the necessary adjustments to maximize impact as the projects evolves.

As part of this strategy, the HORSE team has triggered and maintains a track record of active contribution to various standardization bodies, communities, and associations identified as relevant targets. The standardization task focuses on coordinating with these communities to maximize the impact of technical project results. Additionally, both policy bodies and open-source communities are also monitored, seeking out any relevant fora where the project outcomes can provide valuable contributions.

To coordinate these activities, the consortium standardisation task works closely with the technical activities and experts already engaged in standardization bodies and open-source activities. Partners are committed to identifying and participating in any opportunities to contribute to technical document specifications, working groups, software, proofs of concept, and whitepapers.

Tracking tools for standardisation targets and specific standardisation actions have been made available at the project collaborative repository, so partners can keep track of these actions and coordinated related activities.

Specific potential roles for the partners in the different target group have been identified, shaping the kind of intended contributions:

- **Leadership** implies two have a role in leading the group activity, as a chair position in the group, any of its subgroups, or any supporting board on policy or technology.

- **Editor** corresponds to those roles related to acting as the main author(s) or rapporteur(s) for a specific document, work item or software module.
- **Contributor** is the role of those partners actively contributing to the elements mentioned in the bullet above, whether a document, a work item or a software module.
- **Participant** is associated to those partners taking part in the corresponding activity, regularly participating in discussions and bringing HORSE views and concepts.

For the classification of the standardisation actions a series of categories have also been identified, so a clear understanding of the scope and impact of each individual action can be assessed:

- **Leadership** corresponds to one of the partners being appointed to a leadership position in the target group.
- **Charter** corresponds to the active contribution and/or support to a new activity within a group, or to the creation of a new group.
- **Publication** is associated to the target group publishing the referred standard or software release, after all their formal procedures for acceptance.
- **Contribution** is considered any material proposed to become part of standardization documents and drafts in progress, and code submissions to open-source initiatives.
- **PoC** is associated to a practical demonstration of standards, drafts in development or open-source reference implementations, through public execution of a demonstrator.
- **Presentation** corresponds to any action extending the project outreach in group meetings by introducing HORSE concepts and results.
- **Meeting** covers the active participation in formal group meetings to incorporate project views and outcomes into standards of any nature.

12.3 Standardisation Actions

The tracking tool has registered fifty (50) standardisation actions so far, with their main targets in the IETF and ETSI, in particular on aspects related to:

- The network operations, security, and routing areas in the IETF, on:
  - Lifecycle management
  - Attestation and path trustworthiness
  - Data modelling and accountability
  - Identity management and privacy
  - Workload identities
- Automation and the applicability of AI to network management in ETSI, on:
  - Network autonomy definitions
  - Normative aspects of Network Digital Twins (NDT).
  - NDT integration in management lifecycles.
  - Intent-based management
  - Intent lifecycles

Additionally, the project has contributed to the policy work in GSMA, supporting its work on 6G requirements and on addressing quantum-resistant security services, and to the OSM open-source community, addressing their long-term view and making contributions on NDT orchestration.

As the project plans to have available its first demonstrators, opportunities for proposing PoCs in ETSI (on NDT and AI-enabled security) and the IETF (on NDT integration) are being analysed.

13 Conclusions

The HORSE project has made significant progress in its impact creation activities during the reporting period. The consortium will focus on actively engaging and supporting the adoption and deployment of the concepts and tools offered by HORSE through dedicated promotional activities. To achieve this, the project will participate in events, organise the cybersecurity, and privacy in 6G concepts and trainings to educate stakeholders on the project's outcomes, organise thematic webinars to present the project's results and foster liaisons with relevant initiatives, and organise workshops and demos to engage the research community.

In parallel, further promotional materials, news item, newsletters will be created and distributed. At the same time, the partners will continue to publish scientific publications in renowned journals and conferences. 1. Technical reports showcasing the project's progress. 2. Additional e-newsletters' editions to keep stakeholders informed. 3. Presenting results and lessons learned at relevant events and platforms. By focusing on these activities and measures, the HORSE project aims to create a lasting, sustainable impact on the 6G security and privacy landscape, fostering innovation and promoting the adoption of its concepts and tools across various sectors.

References

[1] T. Hill and R. Westbrook, “SWOT analysis: It’s time for a product recall,” *Long Range Plann.*, vol. 30, no. 1, pp. 46–52, Feb. 1997, doi: 10.1016/S0024-6301(96)00095-7.
[2] “Running Lean: Iterate from Plan A to a Plan That Works - Running Lean, 2nd Edition [Book].” Accessed: Dec. 10, 2024. [Online]. Available: https://www.oreilly.com/library/view/running-lean-2nd/9781449321529/index.html
[3] M. Morrison, *Strategic Business Diagnostic Tools - Theory and Practice*. CreateSpace Independent Publishing Platform, 2013.
[4] “(PDF) Survey on 6G Frontiers: Trends, Applications, Requirements, Technologies and Future Research,” *ResearchGate*, Dec. 2024, doi: 10.1109/OJCOMS.2021.3071496.
[5] “(PDF) Towards 6G wireless communication networks: vision, enabling technologies, and new paradigm shifts,” *ResearchGate*, Oct. 2024, doi: 10.1007/s11432-020-2955-6.
[6] “(PDF) Quantum Machine Learning for 6G Communication Networks: State-of-the-Art and Vision for the Future,” *ResearchGate*, Oct. 2024, doi: 10.1109/ACCESS.2019.2909490.
[7] “6G Market Size, Share | Industry Report [2035].” Accessed: Dec. 10, 2024. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/6g-market-213693378.html
[8] “5G Security Market Size, Share, Trends, Revenue Forecast & Opportunities | MarketsandMarkets™,” MarketsandMarkets. Accessed: Dec. 11, 2024. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/5g-security-market-261636732.html
[9] “Cybersecurity Market Size | Mordor Intelligence.” Accessed: Dec. 11, 2024. [Online]. Available: https://www.mordorintelligence.com/industry-reports/cyber-security-market
[10] G. Zhang, L. Luo, L. Zhang, and Z. Liu, “Research Progress of Respiratory Disease and Idiopathic Pulmonary Fibrosis Based on Artificial Intelligence,” *Diagnostics*, vol. 13, no. 3, Art. no. 3, Jan. 2023, doi: 10.3390/diagnostics13030357.
[11] “Robust and Secure Quality Monitoring for Welding through Platform-as-a-Service: A Resistance and Submerged Arc Welding Study.” Accessed: Dec. 10, 2024. [Online]. Available: https://www.mdpi.com/2075-1702/11/2/298
[12] M. S. Munir, S. H. Dipro, K. Hasan, T. Islam, and S. Shetty, “Artificial Intelligence-Enabled Exploratory Cyber-Physical Safety Analyzer Framework for Civilian Urban Air Mobility,” *Appl. Sci.*, vol. 13, no. 2, Art. no. 2, Jan. 2023, doi: 10.3390/app13020755.
[13] J. Grady, “Trends in Zero Trust: Strategies and Practices Remain Fragmented, but Many Are Seeing Success,” Enterprise Strategy Group. Accessed: Dec. 10, 2024. [Online]. Available: https://www.techtarget.com/esg-global/survey-results/trends-in-zero-trust-strategies-and-practices-remain-fragmented-but-many-are-seeing-success/
[14] “What is Zero Trust and How Does It Work?,” Custom Software Development Company. Accessed: Dec. 10, 2024. [Online]. Available: https://maddevs.io/blog/what-is-zero-trust-network-architecture/
[15] “What Is Zero Trust? | IBM.” Accessed: Dec. 10, 2024. [Online]. Available: https://www.ibm.com/topics/zero-trust
[16] “Network Security Market Size, Growth & Forecast | 2033.” Accessed: Dec. 10, 2024. [Online]. Available: https://www.imarcgroup.com/network-security-market
[17] D. Evans, “How More Relevant and Valuable Connections Will Change the World”.
[18] “Internet of Everything: Meaning, Examples, and Uses,” Spiceworks Inc. Accessed: Dec. 10, 2024. [Online]. Available: https://www.spiceworks.com/tech/iot/articles/what-is-internet-of-everthing/
[19] “The Internet of Everything: Are Connected Things no Longer Enough?,” Intellias. Accessed: Dec. 10, 2024. [Online]. Available: https://intellias.com/what-is-internet-of-everything/
[20] “Software defined solutions for sensors in 6G/IoE | Request PDF,” *ResearchGate*, Dec. 2024, doi: 10.1016/j.comcom.2020.01.060.

[21]"(PDF) 6G Communication Technology: A Vision on Intelligent Healthcare," ResearchGate. Accessed: Dec. 10, 2024. [Online]. Available: https://www.researchgate.net/publication/341451844_6G_Communication_Technology_A_Vision_on_Intelligent_Healthcare
[22]"IoT active connections in smart cities EU 2016-2025," Statista. Accessed: Dec. 10, 2024. [Online]. Available: https://www.statista.com/statistics/691843/smart-city-iot-active-connections-in-the-eu/
[23]"The Future of 5G | IBM." Accessed: Dec. 10, 2024. [Online]. Available: https://www.ibm.com/think/insights/5g-future
[24]m53ber, "WienBot - the digital assistant of the City of Vienna." Accessed: Dec. 10, 2024. [Online]. Available: https://www.wien.gv.at/english/bot/index.html
[25]"State of private 5G in 2024: Key growth trends, use cases, and forecast," IoT Analytics. Accessed: Dec. 10, 2024. [Online]. Available: https://iot-analytics.com/private-5g-2024-key-growth-trends-use-cases-forecast/
[26]V.-L. Nguyen, P.-C. Lin, B.-C. Cheng, R.-H. Hwang, and Y.-D. Lin, "Security and Privacy for 6G: A Survey on Prospective Technologies and Challenges," *IEEE Commun. Surv. Tutor.*, vol. 23, no. 4, pp. 2384–2428, 2021, doi: 10.1109/COMST.2021.3108618.
[27]R. Uddin, S. A. P. Kumar, and V. Chamola, "Denial of service attacks in edge computing layers: Taxonomy, vulnerabilities, threats and solutions," *Ad Hoc Netw.*, vol. 152, p. 103322, Jan. 2024, doi: 10.1016/j.adhoc.2023.103322.
[28]"(PDF) Enhancing Network Slicing Security: Machine Learning, Software-Defined Networking, and Network Functions Virtualization-Driven Strategies." Accessed: Dec. 10, 2024. [Online]. Available: https://www.researchgate.net/publication/381791225_Enhancing_Network_Slicing_Security_Machine_Learning_Software-Defined_Networking_and_Network_Functions_Virtualization-Driven_Strategies
[29]A. Farao *et al.*, "SECONDO: A Platform for Cybersecurity Investments and Cyber Insurance Decisions," in *Trust, Privacy and Security in Digital Business: 17th International Conference, TrustBus 2020, Bratislava, Slovakia, September 14–17, 2020, Proceedings*, Berlin, Heidelberg: Springer-Verlag, Sep. 2020, pp. 65–74. doi: 10.1007/978-3-030-58986-8_5.
[30]Y. Xiao, Y. Jia, C. Liu, X. Cheng, J. Yu, and W. Lv, "Edge Computing Security: State of the Art and Challenges," *Proc. IEEE*, vol. 107, no. 8, pp. 1608–1631, Aug. 2019, doi: 10.1109/JPROC.2019.2918437.
[31]"(PDF) Access control in Internet-of-Things: A survey," *ResearchGate*, Oct. 2024, doi: 10.1016/j.jnca.2019.06.017.
[32]"What Is Quantum Computing? | IBM." Accessed: Dec. 10, 2024. [Online]. Available: https://www.ibm.com/topics/quantum-computing
[33]"Preparing 5G Networks for Quantum Era." Accessed: Dec. 10, 2024. [Online]. Available: https://cpl.thalesgroup.com/blog/encryption/preparing-5g-networks-for-quantum-era
[34]"What is a Zero-Day Exploit? | IBM." Accessed: Dec. 10, 2024. [Online]. Available: https://www.ibm.com/topics/zero-day
[35]M. communications@manageengine.com, "ManageEngine Log360," ManageEngine Log360. Accessed: Dec. 10, 2024. [Online]. Available: https://www.manageengine.com/log-management/
[36]T. H. H. Aldhyani and H. Alkahtani, "Cyber Security for Detecting Distributed Denial of Service Attacks in Agriculture 4.0: Deep Learning Model," *Mathematics*, vol. 11, no. 1, Art. no. 1, Jan. 2023, doi: 10.3390/math11010233.
[37]"Algorithms in Low-Code-No-Code for Research Applications: A Practical Review." Accessed: Dec. 10, 2024. [Online]. Available: https://www.mdpi.com/1999-4893/16/2/108
[38]S. Afrifa, V. Varadarajan, P. Appiahene, T. Zhang, and E. A. Domfeh, "Ensemble Machine Learning Techniques for Accurate and Efficient Detection of Botnet Attacks in Connected Computers," *Eng*, vol. 4, no. 1, Art. no. 1, Mar. 2023, doi: 10.3390/eng4010039.
[39]A. Thakkar and R. Lohiya, "A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research

directions," *Artif. Intell. Rev.*, vol. 55, no. 1, pp. 453–563, Jan. 2022, doi: 10.1007/s10462-021-10037-9.
[40] I. A. T. Hashem *et al.*, "Urban Computing for Sustainable Smart Cities: Recent Advances, Taxonomy, and Open Research Challenges," *Sustainability*, vol. 15, no. 5, Art. no. 5, Jan. 2023, doi: 10.3390/su15053916.
[41] C.-P. Simion, C.-A. Verdeș, A.-A. Mironescu, and F.-G. Anghel, "Digitalization in Energy Production, Distribution, and Consumption: A Systematic Literature Review," *Energies*, vol. 16, no. 4, Art. no. 4, Jan. 2023, doi: 10.3390/en16041960.
[42] "Review of Intelligence for Additive and Subtractive Manufacturing: Current Status and Future Prospects." Accessed: Dec. 10, 2024. [Online]. Available: https://www.mdpi.com/2072-666X/14/3/508
[43] "(PDF) An Overview of Cyber Threat Intelligence Platform and Role of Artificial Intelligence and Machine Learning," *ResearchGate*, Nov. 2024, doi: 10.1007/978-3-030-65610-2_5.
[44] A. Chaddad, J. Peng, J. Xu, and A. Bouridane, "Survey of Explainable AI Techniques in Healthcare," *Sensors*, vol. 23, no. 2, Art. no. 2, Jan. 2023, doi: 10.3390/s23020634.
[45] "Machine Learning Cybersecurity Adoption in Small and Medium Enterprises in Developed Countries." Accessed: Dec. 10, 2024. [Online]. Available: https://www.mdpi.com/2073-431X/10/11/150
[46] D. Preuveneers and W. Joosen, "Sharing Machine Learning Models as Indicators of Compromise for Cyber Threat Intelligence," *J. Cybersecurity Priv.*, vol. 1, no. 1, Art. no. 1, Mar. 2021, doi: 10.3390/jcp1010008.
[47] C. Mironeanu, A. Archip, C.-M. Amarandei, and M. Craus, "Experimental Cyber Attack Detection Framework," *Electronics*, vol. 10, no. 14, Art. no. 14, Jan. 2021, doi: 10.3390/electronics10141682.
[48] "Recent Advances on Federated Learning for Cybersecurity and Cybersecurity for Federated Learning for Internet of Things | Request PDF," *ResearchGate*, Dec. 2024, doi: 10.1109/JIOT.2022.3150363.
[49] "SOK: A Holistic View of Cyberattacks Prediction with Digital Twins | Request PDF," in *ResearchGate*, Dec. 2024. Accessed: Dec. 10, 2024. [Online]. Available: https://www.researchgate.net/publication/378907171_SOK_A_Holistic_View_of_Cyberattacks_Prediction_with_Digital_Twins