REWIRE
Cybersecurity Skills Alliance

Co-funded by the Erasmus+ Programme of the European Union

REWIRE - Cybersecurity Skills Alliance
A New Vision for Europe

R5.2.1 Annual Cyber-security Skills Trends Report

Title	R5.2.1 Annual Cybersecurity Skills Trends Reports
Document description	1st Annual Cybersecurity Skills Trends Report
Nature	Public
Task	T5.2.1 Annual Cybersecurity Skills Trends Reports
Status	Final version
WP	WP5
Lead Partner	MRU
Partners Involved	All
Date	15/03/2023

Disclaimer:

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CONTENTS

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

LIST OF ABBREVIATIONS AND ACRONYMS

Table 1 - List of abbreviations and acronyms

Abbreviation	Explanation/ Definition
ACSC	Australian Cyber Security Centre
CYBERHEAD	Cybersecurity Higher Education Database
EU	The European Union
ENISA	The European Union Agency for Cybersecurity
GDPR	General Data Protection Regulation
IoT	Internet of Things
JRC	The Joint Research Centre
DDoS	Distributed Denial of Service
DoS	Denial of Service
PhaaS	Phishing-as-a-Service
RaaS	Ransomware as a Service
RDoS	Ransom Denial of Service
RFID	Radio-frequency identification
DaaS	Disinformation-as-a-Service
MITM	Man-in-the-middle
NCSC	National Cyber Security Centre (New Zealand)
NTT	NTT Security Holdings
SPARTA CSF	SPARTA Cybersecurity Skills Framework
MITM	Man-in-the-Middle

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

LIST OF TABLES

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

REWIRE
Annual Cybersecurity Skills Trends Report

Summary

An unprecedented increase in the use of the Internet and related technologies has resulted in numerous cybersecurity threats. The cyberspace is subject to an ever-growing variety of attacks, including distributed denial-of-service (DDoS), man-in-the-middle (MITM), web-injection and malicious software attacks, that may take advantage of the new technologies. Recognising and addressing these cybersecurity threats requires a set of specialised skills as well as keeping up with threat development, identifying the main trends and adjusting. The Annual Cybersecurity Skills Trends' Report aims to discuss the status of the necessary cybersecurity skills and gaps to be filled and to present the threats that dominated during the reporting period.

This Deliverable aims to kick off the annual reporting of the status of cybersecurity skills and emerging trends in the EU. The report (this and its iterations) specifically aims to provide insights into the demand and supply of skills in Member State and EU level, trends, mobility of skills, emerging new skills and systematic gaps that require broader action.

The first part of the report addresses the issue of cybersecurity skills gaps. The skills gap analysis is essential for detecting inadequacies of cybersecurity specialist's competencies. The results of the REWIRE stakeholder survey are presented in this report identifying the main deficiencies in cybersecurity skills. As a second step, the results of Concordia, SPARTA, CYBERSec4Europe and ECHO pilot projects' analysis are included to present different perspectives on emerging cybersecurity skills.

The second part of the report addresses the main cybersecurity threats trends identified over the reporting period. To identify the threats trends and cybersecurity risk management practices, several projects have been commissioned by various countries, e. g. New Zealand, Australia, United Kingdom and regional organizations like ENISA. Contemporary cybersecurity risk management practices are driven by compliance requirements, which force organizations to focus on security controls and vulnerabilities. Using the ENISA report as a guide, the report focuses on the threat lifecycle, the various parties involved, and the skills needed at each stage to mitigate the threat. Due to a lack of threat analysis and threat driven skills management, the most impactful threats and vulnerabilities are not properly tackled.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

1. INTRODUCTION

Networked systems are becoming softwarised, and span various application domains, so as to efficiently cater for value creation through digitalization. However, the changes that affect cyberspace and its networked systems and services, such as those due to the evolution of existing technologies or the appearance of new technologies, favour the emergence of new cyber threats that need to be addressed. In particular, the cyberspace is subject to an ever-growing variety of security attacks, including distributed denial-of-service (DDoS), man-in-the-middle (MITM), web-injection and malicious software attacks, that may take benefits from these new technologies, and are orchestrated in a stealthy manner. While they are gaining in sophistication and coordination (i.e., advanced persistent threats), these attacks may affect the fundamental security goals of confidentiality, integrity, availability, and non-repudiation of cyberspace resources. The accessibility, distribution, and increased complexity of networked systems make them particularly vulnerable targets. The nature of cyber threats, which may come from various sources (script kiddies, state hackers, organized criminal groups), is permanently evolving, while the paradigms and technologies are changing.

As “skills gap” we refer to the difference between the skills possessed by the workforce and the skills actually needed to function properly.

To cope with these dynamics inherent to the area of cybersecurity, a systematic method for collecting information on trends, changes and needs is required to be implemented. Through this systematic effort, the 1st Annual Cybersecurity Skills Trends Report aims to identify and anticipate future needs of the Cybersecurity Skills sector and thus provides the accumulated data necessary do develop other deliverables within the Project.

The Report will be structured as follows. Section 2 first details the methodology considered by the Erasmus+ REWIRE project to identify skills trends in cybersecurity. Section 3 describes the status of cybersecurity skills as well as systematic skill gaps, by detailing the results from the Rewire stakeholder survey, as well the results from Rewire dictionary analysis. Section 4 presents the perspectives on emerging cybersecurity skills from the four main pilot projects (Concordia, Sparta, CyberSec4Europe, Echo). Section 5 describes cybersecurity threats trends, and, finally, Section 6 provides threats’ driven need for determining adequate skills in cybersecurity.

This is the first annual cybersecurity skills trends report in this Project. The second annual cybersecurity skills trends report will be delivered at M 36 of the project, and the third one - at M 48.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

2. METHODOLOGY

To construct this report, the project team used a diverse number of information sources. The list in Table 2 depicts the information sources used or planned to be used in the future to support the creation of this report and its iterations.

Table 2 - Skills Trend Report information sources

Information source	Description	Status and Periodicity
Cybersecurity Skills workshop	A workshop for the extraction of early results on the categories of cybersecurity skills was carried out internally.	Implemented (2021 – reported in R2.2.2. Cybersecurity Skills Needs Analysis)
Stakeholders' survey	The Survey conducted to collect information about unfilled cybersecurity job positions, the most sought-after skills and the ability of education providers to train the needed professionals	Implemented (2021 – reported in R2.2.2. Cybersecurity Skills Needs Analysis) Repeated annually
Job Ads Analysis	This tool created by REWIRE team allows identifying, which cybersecurity skills are required within an add and creates appropriate mappings to the relevant cybersecurity roles	In progress - already run on 300+ ads (First results in 2022) The process is ongoing and more results will be extracted before the end of 2023.
The pilot projects (CONCORDIA, SPARTA, CYBERSec4Europe and ECHO)	The information, deliverables and activities of the pilot projects were studied to retrieve their perspective regarding emerging cybersecurity skills	Implemented (2022)
National, regional, European and industry risk and threat reports	Cybersecurity risk and threats reports of various actors (e.g., ENISA), governmental reports (UK, New Zealand, Australia, etc.) and similar are reviewed to provide insights on the subjects of cybersecurity skills.	Implemented (2022) Repeated annually
Sectoral surveys and studies	Sectoral surveys and studies from various organizations (e.g., ISACA, (ISC)^2, Fortinet etc) are reviewed in order to provide further insights on the subjects of cybersecurity skills	Implemented (2022) Repeated annually

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Information source	Description	Status and Periodicity
The CyberABILITY platform	The CyberABILITY platform will combine information and present information to interested parties on the 12 roles of the ECSF, professional courses, academic degrees and certifications.	In progress – will be provided within 2023. At the moment of production of the report, the project team had no data from REWIRE CyberAbility, since it was not ready yet. Therefore, the results of CyberAbility will be incorporated to the second annual cybersecurity skills trends report.

For each skills trend report, the information derived from all these sources, as well as any new identified at that time period, will be combined in order to produce the relevant insights.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3. STATUS OF CYBERSECURITY SKILLS AND SYSTEMATIC SKILL GAPS

The REWIRE partners performed 3 critical steps to identify and analyse information on the cybersecurity skills gap:

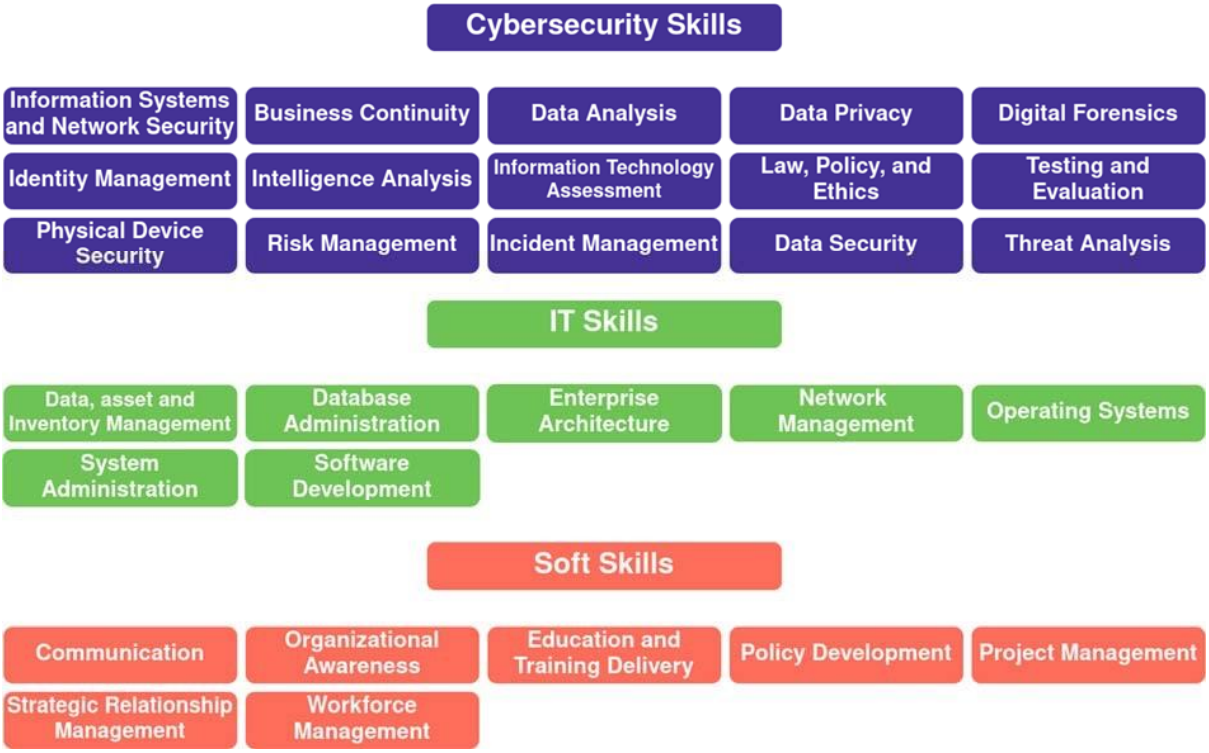
- the implementation of a workshop for the extraction of early results on the categories of cybersecurity skills,
- the implementation of a REWIRE stakeholder survey to get feedback from the project partners and
- the development of a Cybersecurity Job Ads Analyzer. This application has been created to collect and analyse job adverts using a machine learning algorithm which facilitates the identification and mapping of the skills required in advertised open cybersecurity work positions.

Details regarding these actions are provided in the following sections.

3.1. The skills identified for REWIRE analysis

The lack of a commonly adopted cyber security skills framework has been a major threat to objectively identifying and measuring skills needs. To overcome this issue in the project, the REWIRE project designed and implemented a workshop with the aim to classify and structure the NICE framework cybersecurity skills in a way that could be further used for the purposes of the project. This workshop took place in May 2021 with the contribution of all the partners of the REWIRE project. The project partners, took as a base the NICE framework and a taxonomy proposed by the SPARTA project (a set of 57 skills and knowledge) and produced the following categories of skills and knowledge (to be called as REWIRE competencies from now one): cybersecurity skills, IT skills and soft skills. Figure 1 depicts the REWIRE competencies divided per family.

Figure 1 - REWIRE competencies



REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

3.2. Results of REWIRE Stakeholders survey

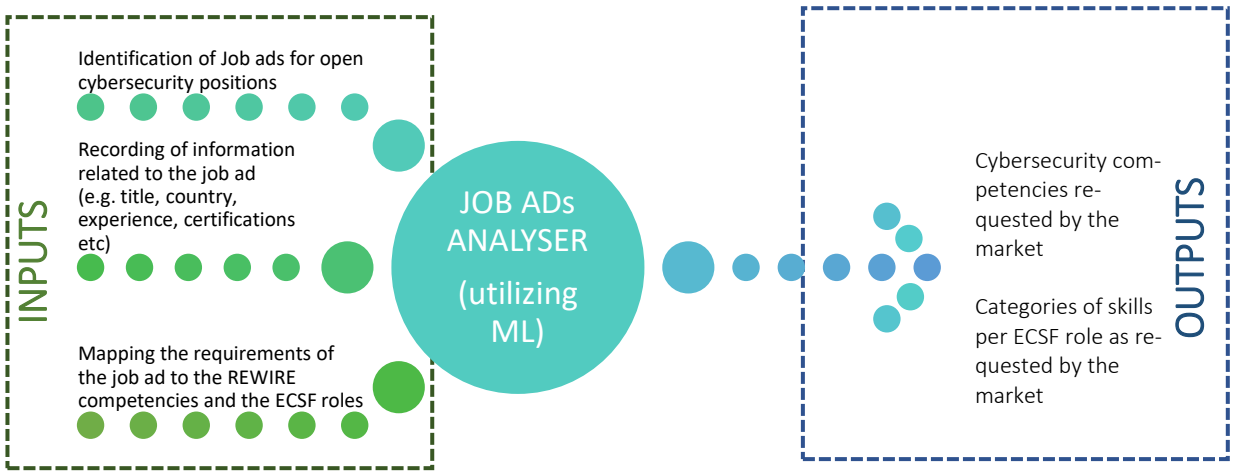
The REWIRE competencies produced from the previous step was used as an input for the stakeholder survey conducted by the REWIRE project. The REWIRE cybersecurity skills survey was created and carried out within WP2 aiming to collect information about unfilled cyber security job positions, the most sought-after skills, and the ability of education providers to train professionals. As part of the REWIRE project tasks, the database of relevant stakeholders was created. The survey was sent out to the contacts identified in the REWIRE stakeholder database in July 2021 and it was officially run until September 2021. In this period, a total of 138 responses from 21 European countries were received. Most respondents were occupied as trainers/professors, but there was a significant number of researchers, managers, consultants, analysts, engineers, and policymakers as well.

The respondents named the following competencies missing from the REWIRE competencies: Secure Development, Application security, SecDevOps. This indicates that the respondents understood that software development is a high-impact discipline that puts insufficient emphasis on secure software development[i].

3.3. Results from Job Ads Analysis

Taking as a starting point the work performed as part of the R.2.2.3. Methodology to anticipate future needs, the REWIRE project has developed and further evolved a tool called Job Ads Analyser. The following diagram depicts the main components and characteristics of the Job Ads Analyser tool.

Figure 2 - Process diagram of the Job Ads Analyser tool



During 2022, the REWIRE project partners, processed 358 Job Ads collected from various, mostly online, digital platforms.

The analysis of the job ads provided two different sets of results.

1. Results regarding cybersecurity skills.

The information from the requirements of the job ads regarding knowledge and skills, has been correlated to the REWIRE competencies mentioned above. This mapping and analysis have been

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

facilitated by a suitably configured and trained ML algorithm. In the end, this process created a top 10 list of most frequently found competencies (see Table 3).

Table 3 - List of most sought-after skills – dictionary analysis

Rank	Skill	Small dataset (Occurrence)	Medium dataset (Occurrence)
1	Network Management	33	83
2	Software Development	34	72
3	Operating Systems		50
4	Policy Development	25	47
5	Information Systems and Network Security	21	44
6	Law, Policy, and Ethics	23	44
7	Database Administration	19	43
8	Threat Analysis	17	38
9	Education and Training Delivery	17	34
10	Strategic Relationship Management		32

The top-down listing shown in the table is ordered by competency frequency in the medium dataset, i.e., based on the frequencies shown in the right-most column. Other competencies found in the small dataset are Communication (19); Workforce Management (19).[ii]

2. Results regarding cybersecurity roles.

The information from the requirements of the job ads, taking into consideration the description of the role requested and the relevant skills and knowledge, was analysed and resulted in a mapping (where possible) to the roles of the ECSF. This way, conclusions regarding which of the ECSF roles are mostly requested by the market (based on the sample of ads analysed) as well as which are other roles requested.

Table 4 - Results of the Job Ads analysis per role

Cybersecurity Roles (in blue background the ones of the ECSF)	**Number of Ads** within analysed sample	**Percentage** within analysed sample
CYBERSECURITY IMPLEMENTER	180	50,28%
CYBERSECURITY ANALYST	34	9,50%
CYBERSECURITY ARCHITECT	26	7,26%
CHIEF INFORMATION SECURITY OFFICER (CISO)	24	6,70%
PENETRATION TESTER	20	5,59%
CYBERSECURITY CONSULTANT	19	5,31%
CYBER INCIDENT RESPONDER	14	3,91%
N/A	8	2,23%
DIGITAL FORENSICS INVESTIGATOR	6	1,68%
APPLICATION SECURITY SPECIALIST	5	1,40%

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

SECURITY OPERATIONS CENTER (SOC) PROFESSIONAL	5	1,40%
CYBER THREAT INTELLIGENCE SPECIALIST	4	1,12%
CYBERSECURITY RISK MANAGER	3	0,84%
CYBERSECURITY RESEARCHER	3	0,84%
CYBER LEGAL, POLICY & COMPLIANCE OFFICER	3	0,84%
CYBERSECURITY AUDITOR	2	0,56%
AI CYBERSECURITY SPECIALIST	1	0,28%
CYBER RANGE SPECIALIST	1	0,28%

*although some ads within the sample appear to be relevant to cybersecurity, after careful examination, it was derived that they were IT roles than Cybersecurity ones.

The above mapping has taken into consideration the alternative titles indicated for each of the ECSF roles within the relevant ENISA publication. (e.g. The CISO has the following alternative titles: Cybersecurity Programme Director, Information Security Officer (ISO), Information Security Manager, Head of Information Security, IT/ICT Security Officer and the Cybersecurity Implementer has the following alternative titles: Information Security Implementer, Cybersecurity Solutions Expert, Cybersecurity Developer, Cybersecurity Engineer, Development, Security & Operations (DevSecOps) Engineer).

The first conclusions that can be drawn from this analysis of this first sample of Job ads are the following:

- The role of the Cybersecurity Implementer is the one identified within half of the examined job ads.
- 11 out of the 12 ECSF roles have been identified within the job ads analysed.
- The role of the Cybersecurity Educator has not been identified within the sample.[1]
- Based on the description of the ads, the tasks identified, and the skills and knowledge requested, a variety of titles have been mapped to the Cybersecurity Implementer role, as indicated from the information included in Table 5. This number of mapped titles is exaggerated also due to the way that the ECSF role has been described (i.e., incorporating various stages from supporting the infrastructure to designing solutions).

Table 5 - Alternative Title of the Cybersecurity Implementer

Alternative Title of the Cybersecurity Implementer (in blue background the ones of the ECSF)	**Percentage***
Advanced Cyber Security Engineer	0,78%
Cyber Security Administrator	0,78%
Cyber Security Applications Expert	0,78%
Cyber Security Engineer	48,84%
Cyber Security Expert	3,10%
Cyber Security Specialist	19,38%
Cyber Security Developer	0,78%
Cyber Security Operations Administrator	0,78%
Cyber Security Professional	2,33%
Cyber Security Specialist	0,78%
Data Security Administrator	0,78%

[1] Conclusions regarding the reason why, can not be drawn at this time due to the limited number of ads analysed. Since more than 1000 ads are planned to be analysed by the end of the year, further conclusions may be drawn then.

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

ICT security specialist	0,78%
Information Security Implementer	2,33%
Information Security Professional	0,78%
Offensive Cyber Security Engineer	0,78%
Operational Technology Security	0,78%
Security Engineer	9,30%
Security Engineering Manager	3,88%
Security Specialist	0,78%
Systems Administrator	1,55%

*This percentage has been calculated against the 180 ads of the sample analysed mapped to the role of the Cybersecurity Implementer.

The same analysis can be depicted also for the second most sought after ECSF role, that of the Cybersecurity Architect.

Table 6 - Alternative Title of the Cybersecurity Architect

Alternative Title of the Cybersecurity Architect (in blue background the ones of the ECSF)	**Percentage***
Cyber Security Architect	33,33%
Cybersecurity Designer	4,76%
Information Security Architect	14,29%
Infrastructure Security Architect	4,76%

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

4. THE PERSPECTIVE FROM THE PILOTS

REWIRE studied various pilot projects to get different perspectives and to help foresee some of the challenges in store. The four main pilot projects studied were Concordia, SPARTA, CYBERSec4Europe and ECHO. These projects mainly focus on identifying shortages of various cyber security skills and job profiles. They also look at the various emerging trends in cyber security. The approach taken involves both quantitative methods like surveying and scrapping social media to more qualitative methods like classifying and scoring various skills. The next sections go through the details of each project and some of their unique aspects.

4.1. CONCORDIA

The CONCORDIA roadmap for Education and Skills aims at covering two main areas: Education for Cybersecurity Professionals[iii] and Cybersecurity Education in high schools[iv].

a) The set of skills are changing as the cybersecurity professionals are expected to have a broader view of the company development, playing a more strategic role, and also include soft skills.

b) The shortage of skills is not only observed in professionals but also in teachers and lecturers. The main reason is that many of them either lack the industry experience or have not been involved in "on-field" projects for a long time. The cyber domain is changing fast, so the people involved in training/education must closely monitor the field and collect as much experience from the real world as possible.

c) Cyberattacks are threatening an increasing range of industries, thus changing the skills needed to perform traditional tasks. The extreme shortage of skills, the complexity of the field, and the associated costs make cybersecurity expertise increasingly costly, which only large companies and organisations can afford. The rest of the digital world (smaller companies, public organisations, etc.) operating on limited resources and employees with little or no background in cybersecurity, are left in a perilous position. For instance, physicians cannot simply take care of the patients but also need to protect their data. The same goes for lawyers who do not only need to understand the cybersecurity field if being a cybersecurity lawyer but also to protect the information they are working with as a significant amount of data is collected during the process. Moreover, the rapid evolution of IT technologies and devices used by the industry (e.g., IoT, digital economy, automation, etc.) and employees (e.g., personal mobiles, wearables, etc.) increase the attack surface and outstrip the skilled employees required to defend them.

d) Among the main challenges of cybersecurity is the interdisciplinarity of the field, which cannot be addressed by just adding another responsibility to IT workers. Cybersecurity is not only about computer science and IT, but also requires good knowledge of the law, social sciences, human factors/psychology, mathematics/cryptography, economics, business planning, etc. It has become a board-level issue, a business risk; hence middle managers and executives would need to understand the importance of the topic and the economic impact of different decisions taken in this respect.

e) As part of a workshop implemented[vii], knowledge and skills are identified for the role of the Cybersecurity Consultant. Specifically, after a series of evaluations the top 10 skills and the top 20 knowledge were identified and insights were provided on the importance of technology knowledge and skills per industry.

The Concordia project demonstrated that elements linked to business economics need to be considered as cybersecurity goes beyond technology and needs to be placed in the broader business context, e.g., when deciding on the investment priorities.

Moreover, the overall technology ranking highlights big data, internet-of-things, and artificial intelligence as major topics of interest, followed by mobile devices and cloud computing. When looking at the knowledge and skills from the perspective of the specific telecom industrial sector, the top-ranked

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

technologies correspond respectively to mobile devices, network softwarization, internet-of-things, followed by cloud computing.

This indicates that when identifying the knowledge and skills of a specific role, the industry where the role is applicable should be taken into consideration.

4.2. SPARTA

The SPARTA roadmap includes the final set of challenges covering emerging challenges; members of the SPARTA consortium consider that these challenges will grow relevant for the EU in the future. The roadmap places the challenges in a timeline specifying short-, mid-, and long-term goals required to complete the challenges[v].

User-Centric Data Governance (in domain of *Data security and privacy* (JRC Taxonomy))

SPARTA consortium considers that connected world experiences be it while surfing the web, using a smartphone, or driving a connected car determines an unprecedented growth in terms of personal, progressively intrusive data collection. Simultaneously, data protection regulation progressed in Europe with the General Data Protection Regulation (GDPR) coming into effect in May 2018 to enhance the protection of the European Union residents in this interconnected world.

SPARTA consortium emphasizes that certain questions related to privacy principles must be understood and defined better. For example, the concept of user control, user empowerment, and user information. Several domains of privacy also require tools. For example, the GDPR presents limited guidance on effectively implementing some of the notions it entrenches, such as Data Protection Impact Assessments (DPIA). In general terms, and irrespectively of GDPR, a wide set of Privacy Enhancement Tools (PET) are necessary, from database anonymization techniques (e.g., required by open-data initiatives) to privacy-preserving protocols of various forms (e.g., for unlikability or anonymized communications). Finally, the absence of transparency in our interconnected world, with various services and devices serving as black boxes, as well as the lack of user control, are considerable issues. How to communicate consent or opposition in the absence of information or user interface? The number, complexity, and diversity of communication technologies and underlying applications prevents identification of such hidden behaviours requiring data flow analyses. Challenging transversal research activities are essential to deliver transparency, emphasize good and bad practices, and empower regulators to enforce data protection laws.

The objective of most activities in privacy is to enable individuals to control their personal data and determine what should be revealed, to whom, and under what conditions. To this end, several dimensions of our connected world must be addressed: at the levels of principle and regulation, at the PET level, and in existing systems.

With the arrival of IoT, privacy leaks may extend to an unparalleled level in volume and precision, within both the digital and physical worlds, and frequently without the knowledge of the user.

Any business must act in accordance with GDPR. Therefore, perception of the concepts, having at our disposal practical tools, having open, accountable, secure, and private-by-design procedures is indispensable. Besides the legal aspect, private companies have a long-term interest to improve their relationship with their clients. In the context of extensive data collection Enhancing trust in the provided products and services is essential for sustainable relationships. The key aspect is delivering transparency, accountability and control to the end-users[vi].

Autonomous Security for Self-Protected Systems

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

SPARTA consortium considers that having a constant and substantial growth in the speed of attack spread or ability to spread, it became essential, firstly, to be able to reveal these attacks in real-time, and secondly, to be able to diagnose these attacks to consider the automatic countermeasures' implementation.

All businesses must protect themselves against potential attacks. Doing so is, however, a difficult and expensive task. The task should be simplified, and the cost reduced by introducing automation. Autonomous security is not presently widely operative. This is the field where Europe should take additional research and consequently industrial lead.

Seeking the idea of autonomous computing, this challenge ultimately pursued the development of computer system qualified to self-manage its own security. The objective is therefore to produce an environment able to correct the security defects by itself in advance.

SPARTA consortium cannot exclude that, even if the feasibility remains an issue temporarily, AI-based systems could manage to autonomously conduct advanced attack campaigns in the coming time. Confronted by automated attacks, a human response could prove to be entirely ineffective. Therefore, the automated response (at least defensively) will be essential. Notably, it will demand some specific actions in the Operational Incident Handling and Digital Forensics domain[vii].

Trustworthy Software (in domains of: *Assurance, audit and certification; Software and hardware Security Engineering; Theoretical foundations* (JRC Taxonomy))

The general challenge is to increase trust in the software security, either through construction or validation. Security in this context means that software respects confidentiality, integrity, and availability of data to be protected. It should be aimed to assemble a comprehensive collection of theories, techniques and instruments that could enhance the trust in the security of our software. To this end SPARTA consortium suggests to develop a course on secure software engineering (incl. both graduate and undergraduate level) that would teach secure-by-design software engineering and certification using the results received from the challenge[viii].

Quantum Information Technology (in all domains)

Industry requires a secure way to communicate and protect its sensitive data. SPARTA consortium believes that quantum computers would jeopardise the existing cryptographic schemas. The new cryptographic schemas must be strong enough to withstand quantum adversary. Moreover, these technologies should also be embedded within the legacy systems. Quantum technology is tempting but should be integrated cautiously in the current classical networks, to secure that all risks are accurately perceived and appropriately addressed.

By itself, quantum computing is an emerging technology, which may soon be implemented in practice. Several cutting-edge cryptographic techniques should be laid out here, for instance, lattice-based, code-based, and multivariate-based primitives.

Training increased numbers of skilful professionals possessing the knowledge of quantum computing and quantum cryptography should, in the view of SPARTA consortium, be prioritized. Additionally, knowledge of quantum theory and information technology should form the basis for the new generation of cybersecurity professionals. These experts shall secure that the integrated quantum-classical IT systems are equally protected from classical, as well as from quantum-related threats, or the hybrid threats[ix].

5G Security (in the following domains: Assurance, Audit, and Certification; Security Management and Governance; Network and Distributed Systems; Software and Hardware Security Engineering; Cryptology). In the following sectors (JRC Taxonomy): Digital Infrastructure, Supply Chain)

SPARTA consortium observes that 5G technology not only provides novel, faster and more trustworthy communication facilities, but also unlocks the opportunity for significantly higher amounts of transferred (sensitive) data, linking various sorts of infrastructures and employing new technologies. The data must be protected from a potential abuse by ill-intentioned technology and software providers as well as dishonest network infrastructure providers.

SPARTA consortium notes that a number of issues require solutions, ensuring suitable protection for the new communication technology, however, the overall goal is to protect the data during its transmission via 5G networks. 5G providers will have to provide for their customers a top level of protection while cooperating with other similar providers assuring divergent level of security. 5G providers relying on (untrusted) 5G technology providers will need assurance that quality of protection will provided, and the solutions applied will be in line with security requirements[x].

Next-generation computing architectures

SPARTA consortium observes that global technical computing progress push into the application domains speedily. Therefore, cybersecurity has to be reinforced to keep up and recover Europe's technical sovereignty in the context of tomorrow's driving technologies. Global supply chains are the source of IoT devices, processors and system-on-chips and it is presently impossible to secure that only trustworthy components are incorporated in neuralgic points of the systems. AI increasingly enhances embedded devices, supported by neuromorphic computing. The computation and the data are currently not adequately protected by corresponding security technologies. High-performance computing is shifting from closed environments to open architectures without taking security into consideration to the necessary extent. Researching new security technologies and their integration into NGC components and systems to ensure European technical sovereignty while leveraging global trends is getting increasingly important. European cybersecurity research and the smartcard industry players are global leaders implicating that substantial security know-how is already available. However, it is problematic to integrate next-generation security technologies for non-security industry into their core components.

SPARTA consortium observes that more and more hardware is created by the open-source community, but it is not ready for commercial use and transfer to the applications in society. The open-source processes and environments for its software, such as Linux, matured over the last two decades. They are now in widespread and productive use, while lately open hardware started to move out of the research community to a widespread industrialisation. Materials for manufacturing are necessary for this process and it has higher turnaround times, meaning that a collective effort and financial support are necessary to proceed with this step and reach maturity enabling European Technological Sovereignty. This, in turn, requires research on designing next-generation open architectures and, beyond that, novel computing platforms based on, for instance, biology or quantum physics[xi].

To conclude, SPARTA project has identified 5G security, data governance, quantum communication, autonomous security as a set of the most critical domains in the upcoming decade.

4.3. CyberSec4Europe

The result from the framework assessment of *CyberSec4Europe* was that the most demanded skills are (in decreasing order of demand) Personal Data Protection and Privacy, Secure Communication

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Protocols, Data Integrity and Authentication, Data Privacy and Access Control. The most demanding profiles are Digital Forensic Analyst, Chief Information Security Officer, Security Operations Centre Manager, Information Security Officer and Software Engineer, whereas the most demanded skill categories over all profiles are Human Security, Data Security, Societal Security, Connection Security and Organizational Security.

After the required skills and their importance (on the scale 0-3) in each of the scenarios were evaluated, *CyberSec4Europe* gathered information from companies involved in the project on the importance of all skills for all professionals described in our framework (in other words, all profiles) based on the rating scale. *CyberSec4Europe* received 6 evaluations and this information was summarized as an average in the final description.

The five most demanded skills (based on the average over all profiles) are: 1) Personal Data Protection and Privacy 2.3; 2) Secure Communication Protocols 2.2; 3) Data Integrity and Authentication 2.2; 4) Data Privacy 2.2; 5) Access Control 2.1.

It is interesting to note that four out of the five most demanded skills are from the Data Security category.

The five least demanded skills (based on the average over all profiles) are: 1) Cryptanalysis 0.6; 2) Customer Service and Technical Support 0.7; 3) Component procurement 0.8; 4) System Retirement 0.9; 5) Component Reverse Engineering 1.0.

CyberSec4Europe notes that the number of answers was quite low, thus all the results were only indicative and might be slightly biased[xii]. To conclude, the CYBERSec4EUROPE project has identified the most demanded skills and job profiles and then proceeded to approach companies to evaluate the importance of each skill for a job profile.

4.4. ECHO

At the time of this report preparation, there are two published ECHO project deliverables related to cyber security challenges – D4.1 *Transversal technical cybersecurity challenges report*[xiii] and D4.2 *Intersector technical cybersecurity challenges report*[xiv].

In D4.1 *Transversal technical cybersecurity challenges report*[xv], transversal technical cybersecurity challenges mean technical cybersecurity challenges that are independent of sector or discipline.

The challenges mentioned in this document were identified through a multistep process of reviewing and analysing the latest cybersecurity reports from a variety of sources, including research, articles and industry reports; then threats and concerns were identified based on the analysis of these reports, and they were then categorised based on already existing taxonomies.

The following transversal technical challenges were identified in this report and listed according to their category:

- Software and Hardware Security Engineering: Application Security (Out-of-date security standards and protocols; Out-of-date and unpatched Windows systems; Attacks on RDP services and Remote Command Execution; DLL Injections; System misconfigurations; Mobile malware; Ransomware); Web Applications (Malicious Browser Extensions; CMS Hacking; Cross-site scripting / XSS Injection; Cross-Site Request Forgery (CSRF); SQL Injection; JavaScript Injection; Crypto jacking scripts and extensions; Fileless and memory-resident malware).

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

- Critical Infrastructures (lack of cyber situational awareness in national critical infrastructure and gaps in defence-in-depth architecture hacking; illicit access to critical infrastructures using IoT flaws and hacking).
- IoT, Embedded systems, Pervasive systems - Access to IoT devices; IoT botnets; Traditional host-centric security solutions are inadequate at protecting IoT devices; Constantly increasing attack surface; Anomalous behaviour is hard to detect; Cross device dependencies; 0-day on CPS.
- Network and distributed systems (Anomalous events of unknown origin in complex systems; Negative effects of complexity and connectivity; Obfuscation as IDS evasion technique; Encryption as IDS evasion technique; Man-in-the-middle attacks; Denial of Service attacks; Encrypted Malicious Web Traffic; Decentralised DNS; False positives in the detection of anomalies, attacks, and intrusion attempts)
- Cloud, Edge, and Virtualisation (Abuse of Cloud Services; Vulnerabilities in cloud infrastructure; Content Delivery Network (CDN) manipulation; Data confidentiality and privacy in cloud environment).
- AI and Big Data Analytics (Adversarial Machine Learning; Malicious use of AI; Disinformation, Fake News, and Deepfakes; Big data security).
- Data security and privacy (Breaches and data leaks; Brute-force attacks; Credential theft; Unauthorised access; Smishing (SMS Phishing); Vishing (Voice Phishing or VoIP Phishing); Data loss; Data tampering).
- Quantum technologies (Conditional security of asymmetric cryptography and fast development of quantum computers (Shor's algorithm); Encryption based on symmetric ciphers with currently using keys can be broken by quantum computer (Grover's algorithm)).
- Incident Handling and Digital Forensics (Attribution of cyberattacks; Lack of proper raw data collection; Lack of dedicated tools to manage cyber threats; Malware Anti-Analysis Techniques; Sandbox evasion techniques; Lack of adequate cyber risk mitigation frameworks) [xvi].

Opposed to D4.1, D4.2 *Inter-sector technical cybersecurity challenges report*[xvii] presents inter sector challenges. It means cybersecurity challenges which are sector-related but span across more than one sectors.

- Software and Hardware Security Engineering: Application Security (PowerShell and VBScript sophisticated backdoors; Living off the land and supply chain attacks); Web Applications (Formjacking);
- Critical Infrastructures (Lack of SCADA/ICS vulnerability assessment tools; Configuration and patch management in ICS/SCADA; Perimeter defence of ICS/SCADA systems)
- IoT, Embedded Systems, Pervasive Systems - Gain access to connected medical devices; Gain access to implanted medical devices; Weak encryption protocols on medical IoT devices; Resource exhaustion attacks on medical IoT devices
- Network and Distributed Systems (Fragmentation as IDS evasion technique; Flooding as IDS evasion technique; Not minding the gap: direct internet connections; Theft, sabotage, and fraud in SIEMs and analytics systems)
- Cloud, Edge and Virtualisation (Hardware vulnerabilities)
- AI and Big Data Analytics (AI in the Military)
- Data Security and Privacy (Credential stuffing attacks; Access to unencrypted data (finance, health records); Unauthorised modification of multimedia content; Ransomware against Electronic Medical Records (EMR); Bio-hacks for multi-factor authentication)
- Incident Handling and Digital Forensics (Lack of SCADA Forensic Tools)
- Vehicular Systems (Detection of rogue or unauthorised autonomous systems; Interference; Transparency and accountability; Unauthorised access to autonomous cars and unmanned vehicles). [xviii]

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

In conclusion, to support the objective pursued by REWIRE, we reviewed cyber security pilot projects and frameworks. The consensus of these projects is that there is a general lack of cybersecurity skills amongst professionals and teachers. Concordia concluded that the lack of skills and increase in cyber treats have necessitated the need for cybersecurity needs to be placed in the context when deciding on investment priorities. SPARTA on the other hand breaks down these goals into short, medium, and long terms goals. They identify sectors like 5G security, data governance, quantum communication, autonomous security as sectors critical over the coming decade. The ECHO project takes a slightly different approach, they classify cyber security needs into 2 categories: inter-sector challenges and transversal cybersecurity challenges. The CYBERSec4EUROPE project starts by identifying the most demanded skills and the most demanded job profiles. It then approaches companies to evaluate the importance of each skill for a job profile. REWIRE aims to expand on these by creating a blueprint that encompasses updating and creating existing and new job profiles. It also targets the identifications of the skills needed based on these job profiles.

5. CYBERSECURITY THREATS TRENDS

A cyber-attack is an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks. There are many types of cyber-attacks. Some of them include phishing, malware, ransomware, DDoS (distributed denial of service), and social engineering. These attacks can cause considerable damage to companies and individuals in terms of productivity, reputation, and theft of sensitive information. With the advent of the internet and portable computing devices cyber-attacks have been on the steady rise. To tackle this, several projects have been commissioned by various countries and regional organizations like ENISA, the NCSC's annual Cyber Threat Report, Australian Cyber Security Centre and the National Cyber Security Centre, UK. These projects publish annual reports of the composition of various cybercrimes in the region or country. Other projects are more focused on specific types of threats. These provide analysis of threat trends in various industries, post-attack analysis and skills development for counter an attack. This section discusses various threat trends and the various projects that study them.

Annually, ENISA produces a status report of the cybersecurity threat landscape based on a methodology[xix] specifying prime threats, major trends observed in connection to threats, threat actors and attack techniques, and also identifies relevant mitigation measures. According to ENISA Threat Landscape report of 2022, the prime threats identified due to their prominence over the reporting period are ransomware, malware, social engineering, threats against data, threats against availability and integrity, disinformation – misinformation, o and supply-chain attacks.

These threats largely correspond to the threats identified in the national reports of analysed states. During the financial year 2020–21, the Australian Cyber Security Centre (ACSC) received over 67,500 cybercrime reports, a nearly 13 per cent increase from the earlier year. The increase of cybercrime reporting in volume compares to one cyber-attack report every 8 minutes in comparison to one every 10 minutes the last financial year. The ACSC categorised a larger number of cyber security incidents this financial year as 'substantial' in impact. This shift is partly due to an increased reporting of attacks on larger organisations by cybercriminals and the observed effect on the victims of these attacks, including some cases of data theft and/or services rendered offline. According to the National Cyber Security Centre of New Zealand (New Zealand NCSC), over the financial year 2020–21, Australian individuals, organisations and governmental institutions' engagement online was significantly impacted by the COVID-19 pandemic. The pandemic has meaningfully increased dependency on the internet of Australians – remote work, accessing information and services, and communicating and continuing with daily lives. This dependence has expanded the surface of attack and brought extra opportunities for malicious cyber actors to pursue vulnerable Australian targets[xx]. According to the National Cyber Security Centre of the United Kingdom (UK NCSC), this year the cyber threat posed to the UK and its

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

partners continued to grow and evolve from indiscriminate phishing scams against mass victims to ransomware attacks against public and private organisations, to targeted hostile acts against critical national infrastructure and government. Although the threats came from a variety of actors employing a multitude of methods, they had one thing in common - they provoked a real-world impact. Lives to-be-saved stolen, critical, and sensitive data compromised, healthcare and public services disrupted, and food and energy supplies adversely affected.

Ransomware as a cybersecurity threat dominates among the top threats in all reports analysed. In Threat Landscape for Ransomware Attacks report, ENISA describes ransomware as an attack type where threat actors take over the control of a target's assets and insist a ransom in exchange for the restoration of the availability of the asset. ENISA observes that this action-agnostic definition encompasses the changing ransomware threat landscape, the predominance of various extortion techniques and the perpetrators' different goals, aside from solely financial gains. According to ENISA, ransomware with few high profile and highly publicised incidents was one of the prime threats in 2022.

In its annual Cyber Threat Report New Zealand NCSC notices a significant tendency in the 2020/21 – incidents of the prominence of criminally motivated activity with an important national impact and potential to cause serious damage. Among the incidents recorded by New Zealand NCSC, 27 % indicated suspected criminal or financially driven actors (increase by 13 % in comparison to previous year)[xxi]. New Zealand NCSC refers to post-compromise incidents covering instances where a malicious cyber actor acquires network access, succeeds in moving through a network laterally, or achieves an effect denying, disrupting, degrading, or destroying the victim's information or system accesses. In the year 2020/21, the post-compromise category covered 33% of malicious incidents. It represents a meaningful increase from the year 2019/20, when only 15% of incidents fell within this category. A significant part of these were denial of service or ransomware incidents. Importantly, denial of service attacks demand long-term business continuity planning and early preparation to evade the consequences of their full impact.

ACSC also observes that ransomware has grown in profile and impact and presents one of the biggest threats to the Australian organisations. In the 2020–21 financial year, the ACSC recorded an increase of 15 % in ransomware cybercrime reports. This increase was related to a growing eagerness of criminals to extort money from most vulnerable and critical elements of society. Cybercriminals' ransom demands varied from thousands to millions of dollars, and their access to the tools and services of dark web improved their capabilities. Extortion tradecraft evolved, with criminals incorporating the victim networks' encryption with threats to release or sell the stolen sensitive data and damage the reputation of victim. Ransomware incidents disrupted a variety of sectors, such as professional, scientific and technical organisations, as well as those in healthcare and social assistance[xxii]. The cybercrime services availability – such as ransomware-as-a-service (RaaS) – via the dark web progressively opens the market up to an expanding number of malicious actors without advanced technical expertise and significant financial investment[xxiii].

According to the UK NCSC Annual Review 2021 report, ransomware became the most significant cyber threat facing the UK this year. It was assessed as potentially harmful as state-sponsored espionage due to the possible impact of a successful attack on essential services or critical national infrastructure. In 2020 the UK NCSC scrutinised the evolving model of criminals exfiltrating data ahead of encrypting victim networks – data which they then threatened to expose unless the ransom is paid (known as double extortion). Therefore, in the last Annual Review, the UK NCSC demonstrated how the ransomware model had drifted from not only withholding data but threatening to make it public as well. The current year, the model has further developed into what is labelled Ransomware as a Service (RaaS), where off-the-shelf malware variants and online credentials are accessible to other criminals for a one-off payment or a share of profits. As reported by UK NCSC, since the business model has become progressively more successful, with these criminal groups securing considerable ransom payments from large businesses which cannot afford to lose their data by encryption or to suffer being offline

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

while their services are down, the ransomware market has become increasingly 'professional'[xxiv]. Ransomware received an increased public attention after the attacks on Colonial Pipeline in the US, which supplied fuel to the East Coast, and against the Health Service Executive in Ireland.[xxv]. According to UK NCSC, in the UK an increase both in the scale and severity of ransomware attacks could be observed. Hackney Borough Council experienced a significant disruption of services – which determined IT systems being down for months and delayed purchases of property within the borough. Attacks this year were over the economy, concentrating on businesses, charities, the legal profession and educational public services, local government and health sectors. A major attack on the American software firm Kaseya was amid other ransomware incidents investigated. In July, the UK NCSC assisted in identifying and supporting British victims after the Florida-based company was penetrated by a hacking group, which seized troves of data and insisted for its return $70m (£51.5m) in cryptocurrency. The UK NCSC welcomed international efforts in tackling ransomware when it was discussed at the G7 meeting of world leaders in Cornwall, emphasizing the necessity for co-ordinated multilateral consideration.

According to The Sophos 2021 threat report[xxvi] more ransomware groups now engage in data theft so they may threaten targets with extortion over the release of sensitive private data. These groups put more effort in organizing more sophisticated attacks. Moreover, these groups are collaborating more closely with their peers in the criminal underground, behaving more like cybercrime cartels than independent groups. As ransomware was identified as one of the most impactful threats, Sophos 2021 Report on Ransomware[xxvii] provides more detailed information on this matter. The report highlights a growing number of ransomware attacks as 37% of respondents' organizations were hit by ransomware in the last year. 54% that were hit by ransomware in the last year said the cybercriminals succeeded in encrypting their data in the most significant attack. The average bill for rectifying a ransomware attack, considering downtime, people time, device cost, network cost, lost opportunity, ransom paid etc. was US$1.85 million. This shows huge rise of ransomware attacks and potential losses to be suffered. Trained IT staff who are able to stop attacks is the most common reason why some organizations are confident they will not be hit by ransomware in the future[xxviii].

In the threat Intelligence Report 2022[xxix] Truesec recommends focussing on early detection of intrusion, meaning substantial capability consisting of functionality for detecting suspicious behaviour, responding to threats and a central console for administration and investigation. Zero-Trust Architecture has to be a standard. The total number of cyber incidents that Truesec handled during 2021 increased by 160% compared to 2020. The Report emphasizes that major ransomware gangs are becoming faster. Constant monitoring of the environment is key to proper cybersecurity. Cybercriminals are efficient at exploiting new vulnerabilities. The growth of DDoS ransom attacks is observed[xxx].

The CrowdStrike 2022 Global Threat Report[xxxi] shows enterprise risk is coalescing around three critical areas: endpoints and cloud workloads, identity and data. The report observes that despite new approaches taken by law enforcement, including attempts to seize ransom payments and criminal funds before they reached adversaries' hands, CrowdStrike Intelligence observed an 82% increase in ransomware-related data leaks in 2021, compared to 2020. This increase, coupled with other data leaks, is a stark reminder of the value that adversaries place on victim data[xxxii].

Malware is the second most prominent threat distinguished in the analysed reports. ENISA defines malware, alternatively described as malicious code or logic, as an overarching concept applied to describe any software or firmware aimed to perform an unwarranted process that will adversely impact a system's confidentiality, integrity or availability. Generally, malicious code types are viruses, worms, trojan horses or other code-based entities that infect a host. Other examples of malicious code include spyware and some forms of adware. According to ENISA, over this reporting period, we again observed many incidents related to malware.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

As reported by New Zealand NCSC, many malicious cyber campaigns fully automate the process of vulnerability scanning, performing initial network breaches, as well as installing malware. These campaigns indiscriminately acquire footing on any vulnerable networks, while the actors return to exploit the targets with highest-value from a set of already-breached networks. The pace of automated exploitation for newly found vulnerabilities is now commonly faster than fixing cycles, even for organisations with abundant resources and commendable security practices. According to New Zealand NCSC, further to patching and maintaining software, organisations also must check for clues of a compromise in all situations in which their network may have been vulnerable, even if for a limited period[xxxiii].

NTT Security Holdings is providing proactive cyber defence and services to customers across the globe. Its 2022 Global Threat Intelligence Report[xxxiv] describes threats identified in 2021 from NTT's perspective. Trojan deployments soar as botnets re-emerge. NTT observed a 50% increase in malware year on year led by trojans and botnets during 2021. Ransomware prevalence impacting business continuity. The most common method attackers use to infect organizations is via email containing malicious links or attachments[xxxv]. NTT observed about a 30% increase in hostile activity targeting clients, led by attacks against applications and network infrastructure, along with denial of service and brute-force attacks. Attack volumes increased for 7 of the top 10 most targeted industries with web-application attacks and application-specific attacks up in most industries and nearly every geographic region[xxxvi]. The Report mostly targeted applications or technology – Apache products (35%), ThinkPHP (8%), Microsoft products (7%), Realtek (5%), PHPUnit (5%). Main target identified in the Report was supply chain as it can cause wide-ranging damages by impacting many organizations as their clients[xxxvii].

Social engineering, as defined by ENISA, encompasses a wide range of activities aiming to exploit a human error or behaviour having the intention to gain access to information or services. It employs many forms of manipulation to deceive victims to make mistakes or hand over sensitive or secret information. In cybersecurity, social engineering baits users to open documents, files or e-mails, visit websites or grant unwarranted persons access to systems or services. And even though these tricks can rely on abusing technology they constantly depend on a human element for success. The following vectors mainly comprise this threat canvas: phishing, spear-phishing, whaling, smishing, vishing, business e-mail compromise (BEC), fraud, impersonation and counterfeit.

According to ACSC, malicious actors used the coronavirus pandemic environment by pursuing Australians' demand for digital information or services. For instance, spear phishing emails were routinely related to COVID-related topics, inviting recipients to insert personal credentials to get access to information or services related to COVID. The health-care sector was also a target of criminal and state actors. In addition, ACSC reports that business email compromise (BEC) remains a serious threat to Australia's businesses and government enterprises, particularly because larger proportion of Australians work remotely. In the financial year 2020–21, the average loss per event has surged to more than $50,600 (AUD) – over one-and-a-half times more than during the last financial year. Cybercriminal groups conducting BEC have possibly grown more sophisticated and organised, and these groups have evolved enhanced, streamlined methods for targeting Australians[xxxviii].

According to New Zealand NCSC, across malicious incidents from the year 2020/21, the technique appearing most commonly was vulnerability scanning, while the most commonly recorded method to acquire initial access to a network was through exploiting a public-facing application. While phishing remains frequent, many organisations have advanced their defences and picked up security products able to scan and manage email traffic well. Majority of contemporary computer users have strong understanding of how to recognise and avoid malicious emails. In response, malicious cyber actors have identified new practices to violate network perimeters and acquire initial access to target networks – exploiting software vulnerabilities is the new preferred access method as witnessed by the

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

NCSC[xxxix]. Notably, user awareness programs should be initiated to combat the continued threat of phishing and related social engineering techniques.[xl]

According to the Sophos 2021 threat report[xli], 70% of survey respondents reported an increase in phishing attacks on their organization since the start of the pandemic. All sectors were affected, with central government experiencing the highest increase (77%), closely followed by business and professional services (76%) and healthcare (73%). The report puts the emphasis on the importance of having a cyber security awareness program in company, to regularly review and update its materials thus ensuring that they are still relevant and engaging for users. In addition, phishing protection tools can decrease the number of phishing emails reaching users and, in that way, decrease the possibility of a successful phishing attack by preventing it at first place[xlii].

Threats against data, according to ENISA, shape a collection of threats targeting data sources to gain unwarranted access and disclosure, as well as data manipulation to interfere with the systems' behaviour. These threats also form the basis for many other threats, discussed in this report as well. For example, ransomware, RDoS (Ransomware Denial of Service), DDoS (Distributed Denial of Service) seek to deny access to data and possibly secure a payment for access restoration. As described by ENISA, threats against data can mainly be categorised as data breach and data leak. Data breach is a purposeful attack launched by a cybercriminal to obtain unauthorised access and release sensitive, confidential, or protected data. Data leak is an incident which can cause an unintended release of sensitive, confidential, or protected data because of, for example, misconfigurations, vulnerabilities or human errors.[xliii] As reported by New Zealand NCSC although denial of service attacks and ransomware incidents can be expensive and have immediate effects on businesses, organizations often have plans in place to recover from them. In contrast, the damage caused by a data breach is more difficult to fix, particularly when the data is a company's most valuable asset. According to the UK NCSC, threat of leaking of the stolen data is almost certain to grow.

CrowdStrike Holdings, Inc. is a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk-endpoints and cloud workloads, identity, and data[xliv]. According to the CrowdStrike 2022 Global Threat Report[xlv], cloud-based services now form crucial elements of many business processes, easing sharing and collaboration. However, these same services are increasingly abused by malicious actors in the course of computer network operations (CNO), a trend that is likely to continue in the foreseeable future as more businesses seek hybrid work environments. Common cloud attack vectors used by eCrime and targeted intrusion adversaries include cloud vulnerability exploitation, credential theft, cloud service provider abuse, use of cloud services for malware hosting and C2, and the exploitation of misconfigured image containers[xlvi]. CrowdStrike Holdings recommends securing all critical areas of enterprise risk: endpoints and cloud workloads, identity, and data; to find solutions that deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. Establishing a strong IT hygiene with an asset inventory and consistent vulnerability management is a must[xlvii]. Additionally, it is emphasized that security teams of all sizes must invest in speed and agility for their daily and tactical decision making by automating preventive, detection, investigative and response workflows with integrated cyber threat intelligence directly observed from the front lines[xlviii]. While technology is clearly critical in the fight to detect and stop intrusions, the end user remains a crucial link in the chain to stop breaches. User awareness programs should be initiated to combat the continued threat of phishing and related social engineering techniques. For security teams, practice makes perfect. Encourage an environment that routinely performs tabletop exercises and red/blue teaming to identify gaps and eliminate weaknesses in your cybersecurity practices and response[xlix].

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Threats against availability and integrity is another threat distinguished by ENISA. Availability is the target of an excessive threats and attacks, amidst which DDoS stands out. DDoS targets system and data availability and, even though it is not a novel threat, it has a substantial position in the cybersecurity threat landscape. Attacks occur when system or service users cannot access relevant data, services, or other resources. This can be achieved by exhausting the service and its resources or overburdening the network infrastructure components. According to ENISA, over the reporting period, threats against availability (alongside ransomware) rank the highest, which signals a shift from 2021 where ransomware was evidently at the peak. Internet use and the free flow of information influences everyone's lives. For many people, internet access has become a necessity to work, study, and exercise freedom of expression, political freedom, and social interaction. This group includes the threats that influence internet availability, such as BGP (Border Gateway Protocol) hijacking.[l]

According to New Zealand NCSC, organisations regularly underrate the damage a cyber incident could have on their capability to provide critical services and functions. Accurately foreseeing and estimating the period it could take to recoup from a compromise is a significant part of understanding a cyber risk and designating resources to govern it. The year 2020/21 illustrated the value an effective incident response and business continuity planning brings. As a result, the best-prepared organisations undertook the approach of a 'not if, but when' to their cyber security planning[li].

Disinformation and misinformation comprise another significant threat category. According to ENISA, disinformation and misinformation campaigns are on the rise so far, triggered by the expanding use of social media platforms and online media. Nowadays, digital platforms are the norm for news and media. For many people, social sites, news and media outlets, also search engines, are currently sources of information. Because of the nature of how these sites operate, which is by drawing people and generating traffic to their sites, the information generating more viewers is usually most promoted, sometimes without its prior validation. ENISA reports, that the war between Russia and Ukraine has revealed new ways to utilize this threat, aiming at people's perception of the situation of the war and the parties' responsibilities. Various motives determine the differences between wrong and intentionally falsified information. This is where the concepts of misinformation and disinformation come into picture.[lii]

As reported by New Zealand NCSC, state-sponsored actors sometimes use disinformation to cause confusion or undermine social cohesion, and malicious cyber actors both rely on and facilitate its spread. During the 2020/21 year, COVID-19-themed disinformation and medical misinformation had a significant impact on cybersecurity as they were used as social engineering tactics. Misinformation was spread through pandemic-themed phishing lures and malware, taking advantage of public fear, interest, and need for information about COVID-19. For example, fake organizations using the World Health Organization's logo claimed to sell cures for COVID-19. Some states have increased their disinformation and political interference efforts, and this trend is likely to continue as the rapid growth of artificial intelligence and access to online services make it easier to spread false information. Technology companies are increasingly taking the lead in monitoring the integrity of online data and designing methods to detect and remove fake or machine-generated content. Disinformation has also been used in recent high-profile campaigns related to democratic processes, such as the 2016 US Presidential Election and the 2017 French Presidential Election. In the context of elections, disinformation poses significant challenges because false information about election processes can undermine public trust and disrupt election administration. Some countries, including Aotearoa New Zealand, have condemned such activity.[liii]

A supply chain attack is the last category of threats indicated by ENISA. These attacks aim at the relationship among organisations and their suppliers. As stated in the ENISA Threat Landscape for Supply

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Chain, an attack is regarded to have a supply chain component if it consists of a combination of at least two attacks. To categorise an attack as a supply chain attack, both the supplier and the customer must be targets. One of the first revelation of this kind of attack was SolarWinds which showed the possible impact of supply chain attacks. It appears that threat actors continue feeding on this source to administer their operations and attain a foothold inside organisations, seeking to benefit from the extensive impact and potential victim base of such attacks[liv].

According to UK NCSC, the software company SolarWinds's compromise and the Microsoft Exchange Servers exploitation emphasized the threat of supply chain attacks. These complicated attacks, where actors targeted less-secure elements - such as managed service providers or commercial software platforms - in the supply chain of economic, government and national security institutions, were two of the most severe cyber intrusions ever observed by the UK NCSC. According to ACSC, malicious actors continue targeting supply chains – especially software and services – to gain access to the vendor's customers. Albeit the consequences of large supply chain attacks – such as SolarWinds – were less severe for Australia, some of organisations were driven to take mitigation measures preventing more serious consequences to their networks. The threat posed by supply chain compromises continues to be high – it is challenging for vendors as well as their customers to secure their networks versus well-resourced actors able to compromise software products of wide usage.

There is a tendency in analysed report to underline the growth of the **state-sponsored actors'** activities. According to ENISA, it is possible that Western or NATO allies, particularly critical infrastructure entities, may become targets of retaliatory actions in response to the sanctions imposed on Russia and the support provided to Ukraine. This may involve the coordination of some pro-Russia cybercrime ransomware groups to carry out damaging operations against Western organizations. Additionally, state-sponsored groups may use existing ransomware types to conceal their activities and create the impression of plausible deniability. According to New Zealand NCSC, in 2020/21, out of the 404 NCSC's recorded incidents 28% showed indications of being connected to state-sponsored actors. The slight reduction in this proportion compared to earlier years possibly represents an increase in the fraction of recorded criminal or financial motivation of incidents. Notably, state-sponsored cyber activity is less prone to disturb services or cause evident harm, and less likely to fall under the public spotlight, yet the impacts on Aotearoa New Zealand's economy and effective international presence are genuine[lv]. Attribution of malicious activity to a specific state is a complex process. The rise in the market of sale and exchange of services, tools, and malware will continue contributing to its complexity. Criminally motivated groups are now capable with such capacities which were previously associated with well-resourced state actors, while some work across jurisdictions or from locations providing safe-havens or tolerating their activity[lvi]. In the year 2020/21, 26% of incidents provided insufficient data to make any determination about the responsible actor or their motivation, therefore recording the suspected actor as unknown. The remaining part of incidents comprised proactive or preventative efforts, false positives, data leaks, or other incidents not related to a suspected malicious actor[lvii]. As reported by ACSC, throughout the reporting period, state-sponsored actors frequently targeted Australia, recognizing it as an important target. These actors utilized a variety of methods to infiltrate Australian networks, aiming to obtain sensitive information that could be used to undermine Australia's competitive edge and compromise national security. Also, state-sponsored actors aimed to obtain access to sensitive information relating to the pandemic, including vaccine research, increasing the threat of cyber espionage to Australia. Analogous concerns were expressed by UK NCSC.

The comparison of cybersecurity threats identified in different reports, demonstrated in Table 9, suggests that the variety of attacks and their kinds has increased significantly in the recent years. Several threats stand out as they were mentioned in almost all reports analysed. These threats include cybersecurity workforce gap, malware and ransomware exploits, privacy, data confidentiality, integrity and availability infringement, identity theft, social engineering, unpatched & outdated software, and insider threats. It is also emphasized in most of the reports that the lack of information sharing, and low awareness of cybersecurity threats of society is also a factor determining greater cybersecurity risk

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

and vulnerabilities in organisations. The variety of threats identified by different actors also underlined the need for common taxonomy, categorisation and vocabulary in the field, as very similar and closely related threats are referred to differently by separate actors. Notably, the more recent reports, underline the importance of uncommon factors to cybersecurity, i.e., geopolitical instability and resulting third party related attacks (as well as attacks by state entities).

6. MOST NEEDED SKILLS TO ADDRESS THE IDENTIFIED CYBERSECURITY THREATS

Contemporary cyber security risk management practices are driven by compliance requirements, which force organizations to focus on security controls and vulnerabilities. This method is not reactive enough to emerging security treads. Due to a lack of threat analysis and threat driven skills management, the most impactful threats and vulnerabilities are not properly adequately tackled. This is evident from the reports mentioned in the previous section. In this chapter we introduce threat driven skills analysis. Using the ENISA report as guide, we focus on the threat lifecycle, the various parties involved, and the skills needed at each stage to mitigate the threat. We also provide analysis into the causes of various threat groups and solutions.

All regional and national Cybersecurity threat trends reports discussed in Chapter 5 indicate the growing number of cybersecurity incidents. Although the analysis of such reports indicates that there is still a lack of uniform and universally accepted terminology in regards of cybersecurity threats among actors in different countries and national entities dealing with cyber threat analysis and reporting do not use and/or analyse the same set of cybersecurity threats, the terminology used therein is the same and it allows to compare and assess cyber security threats flagged within the reports. Most of the threats are relevant to all the profiles identified by in the job adds analysis.

For the sake of clarity and continuity with other EU initiatives, the REWIRE project shall use the terminology of threats provided by ENISA in the ENISA Threat Landscape 2022 report[lviii], which, as indicated in Section 5.1.1 defines the cyber security threats in the following groups: ransomware, malware, social engineering, threats against data, threats against availability (Denial of Service and Internet threats), disinformation – misinformation, and supply-chain attacks. Accordingly, the REWIRE Project shall analyse and indicate the cybersecurity needs that are needed to deal with such cybersecurity threats.

The increasing number of cybersecurity incidents and their real-life consequences for the companies and society serves as the evidence that states do not yet manage or are able to ensure safety in cyber sphere for the cyber users and due to decentralized nature of internet and international character of cybercrime operations the cybersecurity as actual activity is largely left for users themselves.

Moreover, each cyber security threat has a lifecycle (before, during and after), which requires involvement of different cybersecurity actors, different actions and thus – different cybersecurity skills. Therefore, before assessing the cybersecurity skills that are emerging as needed to deal with emerging threats, it is important to identify the lifecycle of cybersecurity threat, cybersecurity actors and their respective actions in dealing with such threat:

Table 7 - The lifecycle of cybersecurity threat

Cyber threat development stage	**Cybersecurity actor**	**Actions to minimize/address Cybersecurity Threat**
Before actualization of incident (threat)	Companies	Internal policies and strategies to address cybersecurity issues; maintaining security of

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

	Policy makers Educators	cybersecurity assets and continuous observance for vulnerabilities. Legal landscape clearly prohibiting cybercrimes and providing legal mechanism to fight them. Knowledge about basic cybersecurity concepts allowing members of society to have a basic understanding about cyber threats and how to minimize them
Cybersecurity incident	Company	Internal policies and strategies on how to deal with cybersecurity incident
Fighting cybersecurity incident	Policy makers / law enforcement	Successful investigation of cybercrime incident and prosecution of perpetrators

During the first stage of cybersecurity threat development a particular cybersecurity incident has not materialised yet, therefore the main actors during that stage are: entities (usually companies, but can also be governments in case of state sponsored cybercrime) for which such cybersecurity threats might be relevant; policy makers, which need to provide regulatory framework ensuring effective legal instruments to fight address threats and educators, who need to provide a general knowledge about cybersecurity tenants. It is during this stage that most of the cybersecurity threats related to social engineering and installation of malware, or particular attacks such phishing can be addressed through education or society in general or users in particular (through company policies).

The second stage of cybersecurity threat development encompasses actions that are needed to deal with cybersecurity incident that has actually occurred (or was identified) and right after its identification. As the main target of cybersecurity threats usually is a company, it is the company that serves as the main actor (N.B. it can also be state, when cybersecurity threats are used for geopolitical reasons), which has to deal with the incident itself, document it, fight it and continue its activities right after the incident. Therefore, the skills needed during this phase on the one hand have to be directed to identifying and fighting the threat; on the other – how to proceed once such threat has materialized (e.g. what steps company employees that are not directly involved in fighting and dealing with cybersecurity incident can/should take, including informing law enforcement agencies, communicating/dealing with ransomware attackers, informing clients and/or suppliers about cybersecurity incident, etc.).

The third stage of cybersecurity threat development includes actions that are (or should be) undertaken to fight a cybersecurity incident. In should encompass all law enforcement actions, which are needed to legally document, investigate and prosecute the cybercrime incident perpetrators. The main actor during this stage is state / law enforcement, which should have sufficient cybersecurity skills to fight cybercriminals.

Furthermore, considering the contents of different cybersecurity threat groups it is possible to differentiate such groups based on the character of prevailing cybersecurity skills that are needed to address such threats. Malware, social engineering and disinformation-misinformation attacks/threats can be minimized/fought without in-depth knowledge or skills in IT sphere, as their main method is deception of individual (group of individuals). Access to initiate ransomware or threats against data, threats against availability or supply chain attacks seem to be based more on IT based vulnerabilities and reducing the threat requires IT skills (although the access can be gained through deception too).

Therefore, insofar the cybersecurity threat is based on deception/misinformation of the user, who then gives access to cybercriminal, the skills, which are mostly needed are the ones related to either education of society (users) on cybersecurity skills related to preparation of company cybersecurity policy containing clear rules that minimize occurrence of threats (or giving access to IT systems) through deception and its compliance. As it was mentioned in New Zealand's NCSC's annual Cyber Threat Report[lix] the threat of successful phishing and malware attacks were not that successful due to

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

knowledge of contemporary computer users on how to recognize and avoid malicious emails. Moreover, as was discussed in Sophos 2021 report on Ransomware[lx] – basic security hygiene is the root cause of many of the most damaging attacks.

Whereas when the cybersecurity threat is based on IT system or software vulnerability, the spectre of skills that are needed to address them are not only much wider (as it encompasses all skills from installation, configuration and maintenance of IT infrastructure, to identification and investigation of or fighting against the of cybersecurity incident), but also indicate automation of processes, such as vulnerability scanning, initial network breaches and installation of malware. As such, the automated cybersecurity threat perpetration processes can be fought using other automated solutions (specialized software) and by using specific skills to configure and maintain company's IT infrastructure in such a manner as to minimize initial automated or subsequent penetration within the system.

It should be noted that the REWIRE project deliverable R2.2.2 Cybersecurity skills needs analysis[lxi] also indicate that Information Systems and Network Security skills are among most thought skills in job adds.

To summarize, due to the lack of a common set of terminology, REWIRE uses the terminology described in the ENISA Threat Landscape 2022 report. REWIRE classifies threats into 7 groups: ransomware, malware, social engineering, threats against data, threats against availability (Denial of Service and Internet threats), disinformation – misinformation, and supply-chain attacks. Recently these threats have been on the rise due to the inefficiencies of the state to deal with them. Cyber security threats have a lifecycle, it is important to identify the lifecycle of cybersecurity threat, cybersecurity actors and their respective actions in dealing with such a threat. These threats can vary based on the target user, the nature of the attack and the end objective. REWIRE takes the approach of deriving skills based on the current threat trend facing the industry.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

CONCLUSIONS

- REWIRE stakeholders' cybersecurity skills survey revealed that such competencies, like Secure Development, Application Security, SecDevOps are missing from the consolidated list of NICE competencies, indicating a high awareness of stakeholders that software development is a high-impact discipline which still puts insufficient emphasis on secure software development. In addition, the skills need analysis unveiled that the top 10 skills obtained using machine learning with those obtained using dictionary analysis significantly overlap. Particularly, Information Systems and Network Security, Operating Systems, Threat Analysis and Communication are among the top 10 most important skills observed in analysis results.
- The comparative analysis of several cyber-security-related pilot projects indicates a general trend of lack of cybersecurity skills amongst professionals and teachers. Concordia project concluded that the lack of skills and increase in cyber treats have necessitated the need for a cybersecurity needs to be placed in the context when deciding on investment priorities. SPARTA project broke down these goals into short, medium, and long terms goals identifying sectors like 5G security, data governance, quantum communication, autonomous security as sectors critical over the coming decade. The ECHO project classified security needs into 2 categories: inter-sector challenges and transversal cybersecurity challenges. The latter being challenges independent of sector of operations and the form sector related. The CYBERSec4EUROPE project identified the most demanded skills and the most demanded job profiles and then approached companies to evaluate the importance of each skill for a job profile. REWIRE aim of creating a blueprint should build on these findings by updating and creating the existing and new job profiles.
- Regional and national cybersecurity threat trends reports indicate the growing number of cybersecurity incidents. Overview these trends showed that in 2021 seven groups of threats are the most concerning. These include ransomware, malware, social engineering, threats against data, threats against availability and integrity, disinformation – misinformation, and supply-chain attacks. Experiences of national cybersecurity institutions also indicate an existing lack of attention to basic security hygiene, crucial role of end-users in stopping the cybersecurity breaches. Therefore, a greater level of cybersecurity requires initiating user awareness programs to combat the continued threat of phishing and related social engineering techniques, as well as a wider spectre of skills from the cybersecurity professionals.

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Table 8 - Comparison of identified threats in various reports

Identified threats	ENISA (2017)[lxii]	(ISC)² report[lxiii]	ISACA report[lxiv]	Global Security Outlook 2022[lxv]	Global Security Outlook 2023[lxvi]
OPERATIONAL TECHNOLOGY THREATS					
Cybersecurity workforce gap		+		+	+
Vulnerabilities of ICS components	+				
Unpatched components	+				
Utilizing of outdated and obscure components	+				
Outsourcing of the third parties to manage and maintain the ICS architecture	+				
Remote access to the corporate network	+	+			
Utilizing external servers for critical infrastructure architecture	+				
Integration of IT and OT networks	+				
INFORMATION TECHNOLOGY THREATS					
Malware exploits	+	+	+		
Ransomware			+	+	+
Privacy Infringement	+	+			+
Identity theft	+			+	+
Compromising of communication equipment	+		+		
Web applications attack	+				
Vulnerabilities in Mobile Applications and payment interfaces	+				
Data Confidentiality, Integrity and Availability	+	+	+		+
Eavesdropping and traffic analysis	+				
DDoS	+				
Social Engineering	+		+	+	+
POS intrusions	+				
Miscellaneous errors	+				
Lack of protective monitoring	+		+		

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE Cybersecurity Skills Alliance
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

Vulnerabilities in automated machines (ATMs, cashier machines, POS intrusions)	+				
Large-scale attacks on IoT (medical devices)	+				
Advanced Persistent Threats (APT)	+		+		
Intellectual property theft	+				
Denial of Service (Dos)	+		+		
DNS Cache Poisoning	+				
DNS Spoofing	+				
Cybersquatting	+				
Typosquatting	+				
Adapting to risks from advances in employee computing technologies (e.g., increased prevalence of sensors, AI, etc.)		+			
Injection flaws			+		
Broken authentication			+		
Broken access control			+		
Cross-site scripting (XSS)			+		
Man-in-the-middle attacks			+		
XML external entities (XXE)			+		
Cryptojacking			+		
Watering hole			+		
Living off the land (LOTL)			+		
Insecure deserialization			+		
SHARED IT THREATS					
Unpatched & outdated software	+	+	+		
Low awareness	+			+	+
Lack of incident reporting	+				
Lack of information sharing	+			+	+
Insider threats	+	+	+	+	+
Risks of emerging technologies like blockchain, AI,		+			

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

VR, quantum computing, intelligent automation, etc.					
Keeping up with changing regulatory requirements (e.g. GPDR, AI regulations, breach disclosure requirements etc.), or their ineffectiveness		+			+
Misinformation and disinformation sowing confusion among executives and the board about cyber risks		+			
Security misconfiguration			+		
Third party related attacks			+	+	+
Infrastructure breakdown due to cyberattack				+	+
Geopolitical instability risk					+
Supply-chain resilience					+
Blackmail due to compromised personal data					+
Falsified or stolen medical data					+

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE Cybersecurity Skills Alliance
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

REFERENCES

[i] REWIRE R2.2.2 Cybersecurity Skills Needs Analysis report
[ii] REWIRE R2.2.2 Cybersecurity Skills Needs Analysis report
[iii] CONCORDIA Workshop on Education for cybersecurity professionals - post workshop report, https://www.concordia-h2020.eu/wp-content/uploads/2020/07/CONCORDIAWorkshoponEducation2020-forpublication.pdf
[iv] CONCORDIA Roadmap for Education & Skills, https://www.concordia-h2020.eu/wp-content/uploads/2021/10/roadmaps-05-Education.pdf
[v] SPARTA roadmap, https://www.sparta.eu/assets/deliverables/SPARTA-D3.2-Updated-SPARTA-SRIA-roadmap-v1-PU-M12.pdf
[vi] SPARTA roadmap, https://www.sparta.eu/assets/deliverables/SPARTA-D3.2-Updated-SPARTA-SRIA-roadmap-v1-PU-M12.pdf
[vii] SPARTA roadmap, https://www.sparta.eu/assets/deliverables/SPARTA-D3.2-Updated-SPARTA-SRIA-roadmap-v1-PU-M12.pdf
[viii] SPARTA roadmap, https://www.sparta.eu/assets/deliverables/SPARTA-D3.2-Updated-SPARTA-SRIA-roadmap-v1-PU-M12.pdf
[ix] SPARTA roadmap, https://www.sparta.eu/assets/deliverables/SPARTA-D3.2-Updated-SPARTA-SRIA-roadmap-v1-PU-M12.pdf
[x] SPARTA roadmap, https://www.sparta.eu/assets/deliverables/SPARTA-D3.2-Updated-SPARTA-SRIA-roadmap-v1-PU-M12.pdf
[xi] SPARTA roadmap, https://www.sparta.eu/assets/deliverables/SPARTA-D3.2-Updated-SPARTA-SRIA-roadmap-v1-PU-M12.pdf
[xii] CyberSec4Europe D6.3 Design of Education and Professional Framework, https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Frame-work_Final.pdf
[xiii] CyberSec4Europe D6.3 Design of Education and Professional Framework, https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D4.1_Transversal-Technical-Cybersecurity-Challenges-Report_v1.0.pdf
[xiv] CyberSec4Europe D6.3 Design of Education and Professional Framework, https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D4.2_Inter-sector-Technical-Cybersecurity-Challenges-Report_v1.0.pdf
[xv] CyberSec4Europe D6.3 Design of Education and Professional Framework, https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D4.1_Transversal-Technical-Cybersecurity-Challenges-Report_v1.0.pdf
[xvi] CyberSec4Europe D6.3 Design of Education and Professional Framework, https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D4.1_Transversal-Technical-Cybersecurity-Challenges-Report_v1.0.pdf
[xvii] CyberSec4Europe D6.3 Design of Education and Professional Framework, https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D4.2_Inter-sector-Technical-Cybersecurity-Challenges-Report_v1.0.pdf
[xviii] CyberSec4Europe D6.3 Design of Education and Professional Framework, https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D4.2_Inter-sector-Technical-Cybersecurity-Challenges-Report_v1.0.pdf
[xix] ENISA Threat Landscape Methodology, https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology
[xx] ACSC Annual Cyber Threat Report 2021, https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf
[xxi] National Cyber Security Center (New-Zeland), https://www.ncsc.govt.nz/assets/NCSC-Documents/2020-2021-NCSC-Cyber-Threat-Report.pdf
[xxii] ACSC Annual Cyber Threat Report 2021, https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf
[xxiii] ACSC Annual Cyber Threat Report 2021, https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf
[xxiv] NCSC Annual Review 2021, https://www.ncsc.gov.uk/files/NCSC%20Annual%20Review%202021.pdf
[xxv] ACSC Annual Cyber Threat Report 2021, https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf
[xxvi] Sophos 2021 threat report (company), https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

[xxvii] Sophos 2021 report on Ransomware, https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
[xxviii] Sophos 2021 report on Ransomware, https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
[xxix] Threat Intelligence Report 2022, https://www.truesec.com/hub/report/threat-intelligence-report-2022
[xxx] Threat Intelligence Report 2022, https://www.truesec.com/hub/report/threat-intelligence-report-2022
[xxxi] The CrowdStrike 2022 Global Threat Report, https://irp.cdn-website.com/5d9b1ea1/files/uploaded/Report2022GTR.pdf
[xxxii] The CrowdStrike 2022 Global Threat Report, https://irp.cdn-website.com/5d9b1ea1/files/uploaded/Report2022GTR.pdf
[xxxiii] National Cyber Security Center (New-Zeland), https://www.ncsc.govt.nz/assets/NCSC-Documents/2020-2021-NCSC-Cyber-Threat-Report.pdf
[xxxiv] 2022 Global Threat Intelligence Report, https://www.security.ntt/global-threat-intelligence-report-2022
[xxxv] 2022 Global Threat Intelligence Report, https://www.security.ntt/global-threat-intelligence-report-2022
[xxxvi] 2022 Global Threat Intelligence Report, https://www.security.ntt/global-threat-intelligence-report-2022
[xxxvii] 2022 Global Threat Intelligence Report, https://www.security.ntt/global-threat-intelligence-report-2022
[xxxviii] ACSC Annual Cyber Threat Report 2021, https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf
[xxxix] National Cyber Security Center (New-Zeland), https://www.ncsc.govt.nz/assets/NCSC-Documents/2020-2021-NCSC-Cyber-Threat-Report.pdf
[xl] The CrowdStrike 2022 Global Threat Report, https://irp.cdn-website.com/5d9b1ea1/files/uploaded/Report2022GTR.pdf
[xli] Sophos 2021 threat report (company), https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophos-2021-threat-report.pdf
[xlii] Sophos Phishing Insight of 2021, https://assets.sophos.com/X24WTUEQ/at/2x7wmj8mf69r86fv3bgwc4tm/sophos-phishing-insights_2021-report.pdf
[xliii] ENISA Threat landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[xliv] The CrowdStrike 2022 Global Threat Report, https://irp.cdn-website.com/5d9b1ea1/files/uploaded/Report2022GTR.pdf
[xlv] The CrowdStrike 2022 Global Threat Report, https://irp.cdn-website.com/5d9b1ea1/files/uploaded/Report2022GTR.pdf
[xlvi] The CrowdStrike 2022 Global Threat Report, https://irp.cdn-website.com/5d9b1ea1/files/uploaded/Report2022GTR.pdf
[xlvii] The CrowdStrike 2022 Global Threat Report, https://irp.cdn-website.com/5d9b1ea1/files/uploaded/Report2022GTR.pdf
[xlviii] The CrowdStrike 2022 Global Threat Report, https://irp.cdn-website.com/5d9b1ea1/files/uploaded/Report2022GTR.pdf
[xlix] The CrowdStrike 2022 Global Threat Report, https://irp.cdn-website.com/5d9b1ea1/files/uploaded/Report2022GTR.pdf
[l] ENISA Threat landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[li] National Cyber Security Center (New-Zeland), https://www.ncsc.govt.nz/assets/NCSC-Documents/2020-2021-NCSC-Cyber-Threat-Report.pdf
[lii] ENISA Threat landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[liii] National Cyber Security Center (New-Zeland), https://www.ncsc.govt.nz/assets/NCSC-Documents/2020-2021-NCSC-Cyber-Threat-Report.pdf
[liv] ENISA Threat landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[lv] National Cyber Security Center (New-Zeland), https://www.ncsc.govt.nz/assets/NCSC-Documents/2020-2021-NCSC-Cyber-Threat-Report.pdf
[lvi] National Cyber Security Center (New-Zeland), https://www.ncsc.govt.nz/assets/NCSC-Documents/2020-2021-NCSC-Cyber-Threat-Report.pdf
[lvii] National Cyber Security Center (New-Zeland), https://www.ncsc.govt.nz/assets/NCSC-Documents/2020-2021-NCSC-Cyber-Threat-Report.pdf

REWIRE - CYBERSECURITY SKILLS ALLIANCE A NEW VISION FOR EUROPE
REWIRE CYBERSECURITY SKILLS ALLIANCE
AGREEMENT NO. 621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union

[lviii] ENISA Threat landscape 2022 report, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022/@@download/fullReport;
[lix] National Cyber Security Center (New-Zeland), https://www.ncsc.govt.nz/assets/NCSC-Documents/2020-2021-NCSC-Cyber-Threat-Report.pdf
[lx] Sophos 2021 report on Ransomware, https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf
[lxi] REWIRE Cybersecurity Skills Needs Analysis, P. 17, https://rewireproject.eu/wp-content/uploads/2022/04/R2.2.2-Cybersecurity-Skills-Needs-Analysis_FINAL_v1.1.pdf
[lxii] ENISA Stock taking of information security training needs in critical sectors 2017 report, https://www.enisa.europa.eu/publications/stock-taking-of-information-security-training-needs-in-critical-sectors/at_download/fullReport
[lxiii] (ISC)2 Cybersecurity Workforce Study 2022, https://www.isc2.org//-/media/ISC2/Research/2022-WorkForce-Study/ISC2-Cybersecurity-Workforce-Study.ashx
[lxiv] ISACA State of Cybersecurity report, https://www.isaca.org/go/state-of-cybersecurity-2022
[lxv] Global Cybersecurity Outlook 2022, insight report by the World Economic Forum, https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf
[lxvi] Global Cybersecurity Outlook 2023, insight report by the World Economic Forum, https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf

REWIRE - CYBERSECURITY SKILLS ALLIANCE
A NEW VISION FOR EUROPE
REWIRE
AGREEMENT NO.
621701-EPP-1-2020-1-LT-EPPKA2-SA-B
Co-funded by the Erasmus+ Programme of the European Union