TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies
Department of Software Science
Centre for Digital Forensics and Cybersecurity

Elif Mihrişah Can 233916IVCM

TRAINING NEEDS ANALYSIS FOR CYBERSECURITY TO THE ESTONIAN SPACE INDUSTRY

Master's Thesis

Supervisor: Adrian Venables, Dr
Co-Supervisor: Anna Mandrenko, MSc

Tallinn 2025

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia Teaduskond
Tarkvarateaduse Instituut
Küberkriminalistika ja Küberjulgeoleku Keskus

Elif Mihrişah Can 233916IVCM

KÜBERTURVALISUSE KOOLITUSVAJADUSTE ANALÜÜS EESTI KOSMOSETÖÖSTUSELE

Magistritöö

Juhendajad: Adrian Venables, Dr
Kaasjuhendaja: Anna Mandrenko, MSc

Tallinn 2025

Author's Declaration of Originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Elif Mihrişah Can

Signature: 

18.05.2025

Abstract

The increasing reliance on space systems and the number of diverse actors utilising space based assets have significantly expanded the threat landscape, resulting in an escalation of cybersecurity risks. Consequently, implementing cybersecurity practices in the space domain has become vital. Despite a growing involvement in space related activities in Estonia, no prior research has assessed the current state of perceived cybersecurity knowledge levels and training needs among professionals working within its space industry. This thesis addresses this research gap by conducting a Training Needs Analysis (TNA), primarily informed by semi-structured interviews with industry experts. The research adopts a mixed-method approach, to gain insights into their cybersecurity knowledge gaps and provide feasible proposals for cybersecurity training based on expert input. Additionally, the research explores challenges specific to the space domain, the evolving cyber threat landscape, and existing cybersecurity frameworks. This thesis provides actionable recommendations for the development of cybersecurity training courses to address knowledge gaps within the Estonian space industry that contribute to its resilience against cyber threats. The results are validated internally by triangulation method and externally by space cybersecurity professionals.

The thesis is written in English and is 93 pages long, including 8 chapters, 13 figures and 6 tables.

Annotatsioon

Kasvav sõltuvus kosmose süsteemidest ja üha mitmekesisem hulk osapooli, kes kasutavad kosmosepõhiseid ressursse, on oluliselt laiendanud ohumaastikku ning toonud kaasa küberjulgeoleku riskide kasvu. Seetõttu on küberjulgeoleku praktikate rakendamine kosmosevaldkonnas muutunud üliolulisekss. Hoolimata Eesti kasvavast osalusest kosmosega seotud tegevustes, ei ole seni uuritud, milline on Eesti kosmosetööstuses töötavate spetsialistide tajutud küberjulgeoleku teadmiste tase ja koolitusvajadus. Käesolev magistritöö täidab selle uurimislünga, viies läbi koolitusvajaduse analüüsi (Training Needs Analysis, TNA), mis põhineb peamiselt poolstruktureeritud intervjuudel valdkonna ekspertidega. Uurimistöös kasutatakse kombineeritud meetodit, et saada ülevaade küberjulgeoleku teadmistest ja puudujääkidest ning pakkuda ekspertide sisendil põhinevaid teostatavaid ettepanekuid küberjulgeoleku koolituseks. Lisaks uuritakse töös kosmosevaldkonnale omaseid väljakutseid, arenevat küberohtude maastikku ning olemasolevaid küberjulgeoleku raamistikuid. Magistritöö annab rakendatavaid soovitusi küberjulgeoleku koolituskursuse väljatöötamiseks, et vähendada teadmiste lünki Eesti kosmosetööstuses. Sellega panustab töö teadlikkuse tõstmisse ja vastupanuvõime tugevdamisse küberohtude vastu. Töö tulemusi valideeriti sisemiselt triangulatsiooni meetodiga ning välimiselt kosmose küberjulgeoleku spetsialistide poolt.

Magistritöö on kirjutatud inglise keeles ning koosneb 93 leheküljest, sisaldades 8 peatükki, 13 joonist ja 6 tabelit.

Acknowledgments

I would like to express my innermost gratitude to everyone who contributed to the completion of this research, and here comes much appreciation.

First, I would like to thank my supervisor, Dr Adrian Venables, for suggesting this topic, for the invaluable guidance, feedback, and continuous support he provided throughout this research. I appreciate the suggestions that Birgy Lorenz made, which improved the study significantly. I am grateful to the professionals and organisations who participated in the interviews and surveys. I dearly appreciate their time and willingness to share their knowledge. Their experiences formed the very foundation of this research. I appreciate the space cybersecurity professionals who read my results and provided their comments.

A special thanks to Erki Valk for nodding his head when asked if the Estonian abstract was clear. I appreciate his wisdom. Thanks to Caleb and Mehmet for being such good friends that I had to express my appreciation for their presence even here.

Lastly, I extend my gratitude gradually from the very bottom of my heart to my family, who have always been my greatest source of strength.

This research could not have been completed without the contributions of all these individuals. Thank you.

List of Abbreviations

ASAT	Anti-Satellite
CARD	Coordinated Annual Review on Defence
CI	Critical Infrastructure
CISO	Chief Information Security Officer
COTS	Commercial Off-The-Shelf
CPS	Cyber-Physical System
CTO	Chief Technology Officer
CVE	Common Vulnerabilities and Exposures
E-ITS	Estonian Information Security Standard
ECSF	European Cybersecurity Skills Framework
ENISA	European Network and Information Security Agency
ESA	Enterprise Security Architecture
ESA	European Space Agency
EU	European Union
EU-SST	European Union Space Surveillance and Tracking
GCR	Galactic Cosmic Radiation
IoT	Internet of Things
IR	Ionizing Radiation
JSON	JavaScript Object Notation
KSA	Knowledge Skills and Abilities
MCASAs	Malicious Cyber Activities Against Space Activities
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NLP	Natural Language Processing
NLTK	Natural Language Toolkit
PESCO	Permanent Structured Cooperation
RAKE	Rapid Automatic Keyword Extraction
RF	Radio Frequency
SATCOM	Satellite Communications
SDA	Space Domain Awareness
SCR	Solar Cosmic Radiation
SCR	Space Cyber Range
SDR	Software-Defined Radio

SDS	Software-Defined Systems
SSA	Space Situational Awareness
SST	Space Surveillance and Tracking
STM	Space Traffic Management
SV	Space Vehicle
TNA	Training Needs Analysis

Terms

Cybersecurity Refers to interdisciplinary practice including psychology, strategy, policy, and standards regarding the security of and operations in cyberspace. It comprises of protecting computer systems, networks, and data from digital attacks, unauthorized access, damage, or disruption. Also, threat reduction, vulnerability reduction, deterrence, international engagement, incident response, resiliency, and recovery policies and activities, including computer network operations, information assurance, law enforcement, diplomacy, military, and intelligence missions as they relate to the security and stability of the global information and communications infrastructure [1, 2, 3].

Cyber Threat Landscape Describes the evolving environment of cyber threats, vulnerabilities, threat actors, and attack vectors. It comprises the identification, analysis, and understanding of current and emerging cyber threats, including their sources, methods, and potential impacts [4, 5].

Critical Infrastructure Refers to the infrastructure including both physical and cyber systems that are essential for national security, economic stability, public health, and safety [6, 7].

National Security Refers to the protection of a nation's citizens, economy, institutions, and critical infrastructure from threats, both internal and external. National security comprises military defense, intelligence gathering, cybersecurity, economic stability, and diplomatic relations [8].

Training Needs Analysis (TNA) TNA serves as the training design process to identify the gap between the current and the desired knowledge, skills, and abilities (KSA) [9, 10].

Table of Contents

List of Figures

List of Tables

1. Introduction

Space systems have become integral to modern society, directly affecting the natural flow of daily life by supporting critical infrastructure and national security [11, 12]. They allow essential services such as global communications, navigation, weather forecasting, and disaster management [13] to function. Furthermore, space-based assets play a critical role in defence and intelligence operations by providing strategic surveillance, reconnaissance, and secure communication channels vital to national security [14]. Cybersecurity is crucial for maintaining the confidentiality, integrity and availability of space operations, as any compromise could significantly weaken a nation's ability to project power and achieve their strategic goals [12, 15, 16]. Satellites contribute to national security by providing safeguarding functions with governments corporations and individuals relying on their services [17, 15, 12]. As a result of technological advancements, the growing trend of digitalisation, and the increasing use of satellites have exposed space systems to a greater risk of cyberattacks [18]. Cyber threats have evolved from Cold War-era electronic warfare to sophisticated attacks on ground and space-based assets, often involving multiple actors comprising nations and non-state actors, including criminal groups and hacktivists [12]. A notable example, the cyberattack on Viasat's KA-SAT network, disrupted satellite internet services across Europe, demonstrating the cascading effects that interference to ground infrastructure can have on satellite communications [19]. Similarly, incidents such as the compromise of NASA's ROSAT X-ray satellite by hackers in 1998 and ongoing espionage activities illustrate the vulnerability of satellite systems to cyber intrusions [20].

In 2024 Estonia became a signatory to the Artemis Accords, an international framework aimed at space exploration [21]. Additionally, new opportunities are emerging for Estonia in the field of space cybersecurity [22] as the European Space Agency (ESA) and the space community introduce new technologies for securing space assets [23, 24]. In particular, the Space Cyber Range (SCR), is a specialised simulation environment designed for testing cybersecurity challenges faced by space assets [25]. This step strengthens Estonia's role in the global space community and also grows opportunities for collaboration within its space sector [26]. However, global space exploration not only brings opportunities, but also challenges within. Deeper integration into international space initiatives presents challenges, particularly the need to establish and maintain cybersecurity practices. Assessing cybersecurity knowledge is essential for understanding current competencies, supporting the space industry to withstand evolving cyber threats.

1.1 Objective, Research Gap, and Novelty

This study aims to assess current cybersecurity competency levels in Estonia and identify potential areas where additional training is necessary. By doing so, the research will provide a foundation for targeted cybersecurity training programme suggestions that support space professionals in Estonia. No prior study has assessed the state of cybersecurity knowledge among professionals in the space sector in Estonia. This study seeks to fill the gap and provide practical recommendations for strengthening cybersecurity knowledge in the industry. To achieve this objective, the study uses a Training Needs Analysis (TNA), which is a process that collects data for identifying and prioritising learning needs within an organisation [27]. This study's significance and value lie in its dual focus. Firstly, it aims to assess current cybersecurity knowledge and develop actionable recommendations tailored to the space industry in Estonia. Secondly, it provides a model for improving cybersecurity capabilities within an emerging national space sector and converts that insight into concrete recommendations. Ultimately, this study aims to help develop a more secure space sector capable of solving the challenges posed by the evolving cyber threat landscape, contributing to global efforts. The insights gained throughout this study may serve as a model for other countries with emerging space industries, providing a novel approach. As no previous research has assessed perceived cybersecurity knowledge within Estonia's space industry, this investigation fills an important gap offering practical applications for improving the sector's resilience.

Corresponding research questions have been formulated to achieve this primary objective:

1.1.1 Research Questions

- RQ1. What is the current perceived knowledge level of cybersecurity among professionals in the space industry in Estonia?
- RQ2. What is the current cybersecurity practice among professionals in the space industry in Estonia?
- RQ3. What training measures can be implemented to improve the cybersecurity knowledge of those working in the space sector in Estonia?

1.2 Problem Statement

Although it is still debated whether space will be considered a critical infrastructure (CI) sector [28], it is acknowledged that modern critical systems and military operations are vital for daily life, and national security relies on space technology [29]. Although the space domain has its own unique issues, new challenges emerge from the intersection of two domains that are different from terrestrial security. These issues originated from the beginning of space exploration, which set the foundation for the development of space technologies. Historically, the main focus was on technical feasibility and mission achievement, with no concern for cybersecurity [15]. The introduction of technical advancements in the last two decades, including the integration of Cyber-Physical Systems (CPS), and the Internet of Things (IoT), has significantly expanded the attack surface for space systems. Furthermore, legacy systems, which were not designed with modern security concerns, continue to be in operation. In addition, regulatory and policy frameworks for space cybersecurity are still evolving, and many countries and organisations are struggling to create industry standards and protocols that can protect space assets. The need to address these cybersecurity concerns becomes increasingly apparent. Protecting the space domain is not just about protecting assets, but ensuring the resilience of critical infrastructure and the competency of professionals that support security and the functioning of modern society. Given these challenges, there is a need for cybersecurity solutions specifically designed for the space industry.

2. Literature Review

This chapter explores the current literature on cybersecurity in the space domain by examining its challenges, frameworks, and threat landscape. This provides a foundation for understanding global cybersecurity efforts in the space domain. This chapter begins by outlining the space domain and broader cybersecurity landscape in the space industry, with attention to the growing threat environment and the strategic role of Space Domain Awareness (SDA) [29]. Building on this foundation, the chapter then explores the cybersecurity principles [15] that guide the design and protection of space systems. This is followed by a description of the unique environmental, operational, and cybersecurity challenges within the space domain that influence the complexity of securing these systems. Specific cybersecurity challenges faced by space systems [11, 30] are examined, highlighting the unique operational and structural characteristics that differentiate them from traditional IT systems. For a deeper contextual understanding of cybersecurity frameworks [31, 32, 33] for competency, the chapter also examines relevant cybersecurity workforce competency models. The chapter then examines the TNA process [34] for designing the assessment process that forms the central aim of the study.

2.1 The Space Domain

Space is vast, largely unregulated, and increasingly contested [35]. Historically, space was viewed as a domain for scientific exploration. Progressively, this view is evolving into a critical area for national security, economic growth, and geopolitical influence [36]. The increasing use of space technology for communication, navigation, and surveillance highlights the strategic importance of the space domain, encouraging nations to prioritise space capabilities [37]. The absence of proper international regulations creates risks, as the current regulatory landscape does not clarify terminologies. In addition, it is argued that current international law cannot handle Malicious Cyber Activities Against Space Activities (MCASAs) [38]. Without effective governance and clearly defined regulatory frameworks, geopolitical tensions and operational risks will continue to increase in the space domain [39].

2.2 Challenges in the Space Domain

Working in the space domain presents both environmental and operational challenges, many with unknown probabilities that could destroy a Space Vehicle (SV). Physical risks

apply to SVs regardless of their orbit or function. The first environmental risk to consider is radiation. Space is one of the most extreme environments, with SVs being exposed to different sources of ionising radiation. These can present a significant challenge to both human space exploration and the operation of spacecraft [30, 40]. Three main sources of radiation affecting SVs are Galactic Cosmic Radiation (GCR), Solar Cosmic Radiation (SCR), and Planetary Trapped Radiation, known as the Van Allen Radiation Belt [40, 41]. Each of these radiation types can have detrimental effects, with high doses of radiation able to destroy electronic and electrical systems in space vehicles or satellites. Other concern is temperature, as changes in temperature tend to be more irregular in deep space when compared to an SV in regular orbit due to differences in atmospheric density. For SVs operating in deep space farther from the surface of the earth, fluctuations in the temperature are harder to predict considering the data available. Thus, the risk decisions and preparations become harder for spacecraft and its missions [30]. Another risk regarding the environment is collisions. The risk of collision with space debris or other operational satellites is a growing concern, as the orbital environment becomes increasingly crowded [12]. Operators must make risk-based decisions regarding a collision avoidance, which can be complicated by the absence of clear legal frameworks for liability and manoeuvring responsibilities. The vacuum of space presents further challenges; off-gassing, and sealed components must be carefully managed, as trapped gases can escape or cause damage in the low pressure environment [30]. Another concern is gravity, which is a fundamental challenge in both the launch and operation of SVs. Achieving and maintaining a stable orbit requires precise calculations. While gravitational effects are well understood for Earth-orbiting missions, they become more complex for missions as they go further from Earth. Other challenges represented by the space domain are operational, which are faced during the development and operation of space systems. While environmental factors may exhaust the physical endurance of the SV, operational challenges are about successfully executing the mission over the system's lifespan and are not caused by the domain itself. The first operational challenge to mention is testing, as extensive testing is required to validate an SVs ability to survive and operate in space [30]. This includes environmental testing for temperature, vacuum, radiation, and vibration. Testing is resource intensive and it requires specialised facilities. The launch phase introduces additional risks, including exposure to intense vibrations and the potential for launch vehicle failure. Deployment is an another challenge; the SV must successfully detach from the launch vehicle and begin operating independently. If the separation mechanism fails, the SV may become damaged, making it impossible to operate. After deployment, SVs often require stabilisation to achieve the correct orientation and attitude for mission operations. This process, known as detumbling, consumes onboard resources such as electrical energy or propulsion fuel. Power management presents issues, which are a critical constraint for SV operation and its survival. The energy budget, determined by power generation and consumption determines

the SV's ability to perform mission tasks. Also, electromagnetic emanations from the SV itself can interfere with onboard sensors or ground communications. Testing for emanations is challenging, because it's difficult to replicate the conditions of space on Earth. Anechoic chambers are used for emanation testing, but access is limited and costly. Radio Frequency (RF) management is essential for reliable communication between the SV and ground stations. Frequency selection impacts antenna design, signal reliability, and bandwidth. Regulatory compliance is required to avoid conflicts with other users, and frequency registration must be completed early in the design process. RF challenges are compounded by signal pollution on Earth, which can interfere with ground communications. Another operational challenge posed due to the growing number of space debris, which is de-orbit. SVs must be designed to ensure they can safely de-orbit and burn up in the Earth's atmosphere at the end of their operational life. This adds further complexity on the overall system design [30].

2.2.1 Cybersecurity in the Space Domain

Space systems were primarily designed focusing on functionality rather than cybersecurity [15]. Early space systems were analogue devices and operated in isolated environments with limited connectivity, which directly reducing possibilities for cyber threats. This minimised the need for cybersecurity considerations during the design phase [15]. However, the evolution of space technology (e.g. reliance on Software-Defined Systems, and IoT) has expanded the cyber threat landscape [42, 43, 44]. Although the intersection of space and cybersecurity is not a new topic, it has not been widely recognised as a potentially significant threat, and has been largely neglected [45, 24].

Today, satellites and ground infrastructure are interconnected through complex communication networks, making it vulnerable to cyberattacks (e.g. unauthorised access, signal spoofing, and Denial-of-Service attacks) [46, 47]. Incidents such as reported interference with satellite communications and GPS signal disruptions [48] highlight the need for cybersecurity integration into modern space system designs. Whereas early space systems operated without cybersecurity considerations, the current nature of space systems necessitates proactive cybersecurity integration throughout the design phase [49, 50, 51]. Additionally, numerous studies highlight the necessity and importance of international collaboration and standardised cybersecurity frameworks and regulations in the space domain [52, 53, 38].

2.2.2 The Growing Cybersecurity Threat Landscape

Historically, satellites have relied on security through obscurity, where the complexity of systems and high costs of attacks deterred all but the most advanced adversaries [12, 54, 46]. However, the widespread use of Commercial Off-The-Shelf (COTS) components (ready-made products, including software and hardware) and the rise of constellations with thousands of identical satellites suggest that this level of diversity and complexity in satellite design may not last [46]. Also, space cybersecurity concerns were mainly focused on electronic threats between the United States and the Soviet Union during the early years of the space race [12, 55]. Advancements in space-based technologies have affected the nature of cyber threats, expanding the cyber threat landscape in space [18, 12, 46]. Today, thousands of operational satellites are in orbit in addition to millions of pieces of space debris [12]. This growing congestion is compounded by the increasing participation of both public and commercial entities in space activities, resulting in increased competition [56]. Furthermore, space has become a contested domain, with geopolitical tensions demonstrated through a series of Anti-Satellite (ASAT) tests and hostile space manoeuvrers conducted by states. These activities contribute to a volatile security environment in which the risk of conflict and disruption to space assets have significantly increased [57].

The number of cyberattacks on space systems has also notably risen [12] within the evolving cyber threat landscape, reflecting its growing complexity and vulnerability. Identifying precise numbers is difficult, as most space companies were formally defence companies that operated under a strategy of security through obscurity, hesitant to publish data [12]. However, available data has illustrated a significant increase in the number of cyberattacks targeting space systems. For instance, the Pavur and Martinovic database reports 113 cyberattacks between 1957 and 2022, while CyberInFlight's report identifies 337 incidents since the 1970's [12]. However, according to NASA, more than 6,000 cyber-attacks were experienced only in a 4 year period [58]. These statistics, while useful, likely represent an underestimate of the actual threat landscape, as many incidents continue to go unreported [12].

The cyber attacks also highlight different motivations behind them. Though the general motivation for harming satellites and the profile of threat actors differ, Table 1 presents an overview of these threat actors and their motives [46].

Table 1. Overview of Threat Actors and Their Characteristics in Space Security Literature [46]

Threat Actor	**Primary Objective**	**Capability**
Military	Space dominance, ASAT	Extremely high
Intelligence	Espionage, Counter intelligence, Eavesdropping	Extremely high
Industry Insiders	Sabotage, Intellectual property theft	High
Component Suppliers	Malicious interference, Supply chain attacks	Moderate
Criminal Organisations	Data interception, Ransom demands	Moderate
Terrorist Groups	ASAT, Propaganda	Low to moderate
Business Competitors	Industrial sabotage, Corporate espionage	Low
Hackers	Gaining recognition, Personal achievement	Very low
Activist Groups	Spreading messages, Ideological influence	Very low

2.3 Cybersecurity Challenges to Space Systems

Similar to other technologies, space assets were initially analogue devices. As these analogue systems lacked remotely-accessible software and code vulnerabilities, they did not offer opportunities for malicious remote access. Although space assets digitalised as most systems did as technology developed, cybersecurity was not considered a priority [15]. With the increasing development of space-based systems, cybersecurity professionals encounter threats and vulnerabilities different from those typically observed in operations in the ground segment [59].

2.3.1 Unique Characteristics of Space Systems

Space operations require specialised cybersecurity approaches to ensure secure and resilient systems in an evolving threat landscape [59]. Several factors differentiate cybersecurity in

space from ground-level cybersecurity. Firstly, space represents a globally-accessible and shared domain utilised by both government and private sectors. Due to substantial costs and extended deployment timelines, space-based network architectures struggle to adapt to emerging cybersecurity threats. The physical infrastructure of space systems, designed for prolonged operational lifetimes, leaves these assets vulnerable to cyber threats and hardware degradation after deployment. Finally, smaller space systems, often constructed using COTS technologies due to budget constraints, typically lack integrated cybersecurity protections [59].

2.3.2 Composition of Space Systems

Space systems consist of four main segments: Space, Ground, Link, and User. Each role is essential to the operation and functionality of space assets. Each segment faces various cybersecurity risks, including threats that may originate in one segment and subsequently result in others [59].

2.3.3 Space Domain Awareness (SDA)

The space domain is becoming increasingly recognised as congested, contested, and competitive [60]. However, only a limited number of European Union (EU) Member States have developed and deployed space situational awareness (SSA) capabilities [29]. These capabilities are primarily national demonstrators or secondary functions of assets not originally designed for SSA purposes. These members participate in various multinational initiatives, notably the EU Space Surveillance and Tracking (EU-SST) framework [61], which provides essential services such as collision avoidance, re-entry analysis, and fragmentation analysis. The private sector in Europe is emerging as a provider of space surveillance and tracking (SST) and SSA services, including for national defence purposes. Despite these efforts, the EU and its member states currently lack a comprehensive SSA capability that would ensure secure space activities. Developing such capabilities, alongside EU-SST services will be required to establish a European approach to Space Traffic Management (STM) [62] and address the security and defence challenges outlined in the EU Space Strategy [29]. Within the framework of PESCO (Permanent Structured Cooperation), five Member States are engaged in the European Military Space Surveillance Awareness Network, which aims to set an independent and sovereign EU military SSA capability [29]. Additionally, from the perspective of the Coordinated Annual Review on Defence (CARD), the development of SSA architecture and systems has been identified as a medium- to long-term objective that could be pursued collaboratively [29].

2.3.4 Industry Professionals Perspective

The White House has published an industry perspectives report, highlighting common perceptions of professionals on cybersecurity. The paper shows that the sector faces significant cybersecurity challenges arising from various factors. Common perspectives identified in the report are presented above [63]:

The first topic identified in the report is the inconsistency and fragmentation of cybersecurity requirements within the space industry. From the perspective of space industry professionals, cybersecurity requirements for the space industry are fragmented and inconsistent in government cybersecurity guidelines, both for commercial and government-contracted projects. Many in the space industry view government guidelines as unclear. As a result, companies often develop their own cybersecurity standards and requirements during the design phase, based on their interpretation of existing frameworks and guidelines [63].

The second topic identified is the lack of cybersecurity operations technologies for space missions. It is perceived that typical terrestrial defence tools are not suitable for space operations, as they do not have the necessary accuracy, resource efficiency, or maintenance standards [63].

Next, the third topic identified is that fitting cybersecurity features onto legacy space systems would be too difficult. As legacy space systems were built without cybersecurity concerns, addressing vulnerabilities in these systems would be too difficult and costly. Compliance would involve not only the space industry, but the government as well [63].

The fourth topic is that perceptions on cybersecurity and space missions are disconnected. According to cybersecurity professionals, space industry professionals often see cybersecurity as an obstacle for mission development. Space professionals are also not motivated to invest in cybersecurity without customer demand. This shows the importance of cybersecurity awareness [63].

Another topic identified from the report is improving cybersecurity operations by increasing compliance. Voluntary guidelines are not sufficiently motivating companies to invest in minimum cybersecurity requirements. This implies that regulations and policies are required. Without enforcement, companies can choose whether or not to implement these measurements, often resulting in inconsistent adoption [63].

The next topic identified is that there is too much focus on compliance and understanding existing requirements, rather than implementing cybersecurity practices. According to

space industry professionals, substantial effort is required to understand and adhere to a variety of cybersecurity frameworks, which may not always be relevant to space systems. As a result, compliance activities are seen as detracting from productive activities [63].

Another topic is the inconsistency of the cyber threat information in the space industry, also unactionable. Many space companies experience varying access to cyber threat information, with disparities between larger and smaller organisations. Furthermore, when threat intelligence is received, it may not necessarily be useful or timely enough to take an action [63].

Another topic identified is about space startups. Due to their flexibility and smaller size, space startups are perceived to have an advantage in incorporating better cybersecurity principles. Smaller companies expressed their ability to adopt modern methods of implementing cybersecurity measures, such as using secure software languages during the development phase. However, such implementations can be perceived as a choice between achieving the fundamentals and applying pragmatic cybersecurity measures. Some reported that unless mandated, the primary motivation is proving the products' viability to investors, rather than cybersecurity. Additionally, smaller firms may lack awareness in cybersecurity, especially in the system design phase [63].

Next, another identified topic is lacking expertise and workforce at the intersection of aerospace and computer engineering. Space industry professionals highlighted the limited workforce with interdisciplinary knowledge in computer science and aerospace engineering to ensure that space missions have proper cybersecurity measures implemented by design [63].

Another topic identified in the report concerns software and technology supply chain risk management. Space industry contractors are concerned about cybersecurity risks within their supply chains, including those introduced by subcontractors. However, they also acknowledge that larger companies often fail to clearly define cybersecurity requirements from their subcontractors, making it difficult to manage these risks effectively. As a result, lower-tier vendors may not implement adequate security measures, increasing the overall risk in the supply chain [63].

2.4 Cybersecurity Principles for Space Systems

The importance of understanding cybersecurity principles for space systems is vital for analysing cybersecurity vulnerabilities, protecting critical infrastructure, and addressing the evolving threat landscape [15]. The first space cybersecurity standard that addressed

supply chain cybersecurity for space systems was published by the Aerospace Industries Association in 2013. Although this standard has been widely adopted, only limited further guidance has been released since initial publication [15].

According to Space Policy Directive-5, space systems and their supporting infrastructure should be designed and developed using cybersecurity practices [64]. These systems must continuously monitor and adapt to evolving cyber threats capable of compromising their operations. Owners and operators should develop comprehensive cybersecurity measures to ensure the confidentiality, integrity, and availability of critical functions, missions, and data. Effective supply chain risk management practices, including sourcing from trusted suppliers and identifying malicious components, should also be integrated [64]. Furthermore, stakeholders of space systems should collaborate to develop and share best practices, threat intelligence, and incident information within the industry, consistent with applicable laws [64].

2.5 Cybersecurity Standards and Frameworks

Several international cybersecurity standards and frameworks provide guidance for managing cybersecurity risks. The ISO/IEC 27001 standard outlines requirements for implementing, maintaining, and continually improving information security management systems [1]. The National Institute of Standards and Technology (NIST) Cybersecurity Framework provides a structured approach towards managing cybersecurity risks in critical infrastructure sectors [2]. Additionally, the European Union Agency for Cybersecurity (ENISA) has published guidelines specifically addressing cybersecurity challenges in space infrastructure, particularly emphasising the importance of tailored cybersecurity training and capability development [65]. The European Space Agency (ESA) also provides cybersecurity policies and guidelines tailored to the unique operational context of space missions and infrastructure [66]. These standards and frameworks collectively inform best practices for cybersecurity training and risk management in specialised industries.

2.5.1 Cybersecurity Skills Framework

ENISA introduced the European Cybersecurity Skills Framework (ECSF), which can be applied in a modular and flexible way based on the needs of different stakeholders. The ECSF is designed to create a common understanding of cybersecurity roles, competencies, skills, and knowledge across EU Member States. ECSF helps to address the cybersecurity skills shortfalls by using the recognition of cybersecurity related competencies [32].

A basic orientation is provided by a five step guide as follows [32]:

1. **Analyse the current state.**
   Collect and analyse the data related cybersecurity condition of the environment. Identify goals and parties involved.
2. **Set clear goals.**
   Look at the result of the data analysis, and specify its cybersecurity requirements to be met.
3. **Select the components.**
   Examine the ECSF profiles[1] and choose a profile that applies to a specific situation. Choose the components that help meet the needs of the intended environment.
4. **Adapt the chosen components**
   Make the necessary adjustments for the targeted environment.
5. **Apply the tailor components into the intended environment.** Apply the tailored components to address objectives related to cybersecurity, which are necessary to improve the state of the target environment.

Table 2, presents the ECSF applications that correspond to the five phases [32]:

Table 2. The ECSF Modular Approach in practice [32]

Example	Step	Description
Employing cybersecurity experts	1. Analyse	Analyse the current state of cybersecurity level in the organisation.
	2. Identify	Identify the lack of personnel to handle the increase in cybersecurity issues.
	3. Select	Select the suitable task from an ECSF profile that corresponds to an identified gap in specific skills.
	4. Adapt	Combine the ECSF profiles with tasks of interest to the organisation and structure new roles, skills and knowledge to meet the organisational needs and create cybersecurity roles.
	5. Apply	Use the profile generated to create job vacancies targeted on the specific needs of the organisation.

[1]12 cybersecurity professional role profile presented by ECSF include: Chief Information Security Officer (CISO), Cyber Incident Responder, Cyber Legal, Policy, and Compliance Officer, Cyber Threat Intelligence Specialist, Cybersecurity Architect, Cybersecurity Auditor, Cybersecurity Educator, Cybersecurity Implementer, Cybersecurity Researcher, Cybersecurity Risk Manager, Digital Forensics Investigator, and Penetration Tester [32].

Example	Step	Description
Upskilling cybersecurity experts	1. Analyse	Understand the business objectives and strategy of the organisation.
	2. Identify	Identify any lack of expertise and personnel in areas regarding to cybersecurity.
	3. Select	Use the ECSF profile(s) to identify the associated skills and knowledge that the organisation lacks.
	4. Adapt	Analyse selected skills and knowledge from the ECSF to identify the training needs of a cybersecurity professional to meet the organisation's needs.
	5. Apply	Identify training to improve the competence of the organisation's workforce.
Making career choices	1. Analyse	Choose a career path that you are interested in.
	2. Identify	Identify your skills and the knowledge gap required to move into the cybersecurity sector.
	3. Select	Identify the ECSF profile(s) that you find useful from the perspective of career development, and use the connected skills, knowledge and competences as guidelines for reskilling and upskilling.
	4. Adapt	Improve the selected ECSF profiles by including additional skills and knowledge based on individual needs.
	5. Apply	Identify a training programme applying the majority of the skills and knowledge development required to reskill or upskill for the profile.

2.5.2 The Cybersecurity Competencies Framework

This framework provides a structured approach to identifying and mapping the necessary competencies in cybersecurity. It supports workforce development and training programmes in the cybersecurity sector. The framework categorises competencies into specialised areas such as risk management, incident response, and technical and organisational competencies [33]. Table 3 illustrates the key definitions used by the Cybersecurity Competencies Framework.

Table 3. Key Definitions from the Cybersecurity Competencies Framework [33]

Term	Definition
Role	Performed function in the organisation.
Competency	Set of professional capacities useful to perform tasks.
Task	Activity aimed at achieving functional objectives within the organisation.
Knowledge	Set of associated concepts, memorable, intelligible, and communicable.
Skill	Practical knowledge, ability to perform an observable action.
Cyberspace	Consists of the complex environment of values and interests, in an area of collective responsibility that results from the interaction between people, networks, and information systems.
Cybersecurity	Consists of a set of prevention, monitoring, detection, reaction, analysis, and correction measures and actions that aim to maintain the desired security state and to ensure confidentiality.
Cyberdefence	Consists of the activity that aims to ensure national defence.
Cybercrime	Facts corresponding to crimes defined in the Cybercrime Law and other criminal offences committed with the use of technological means.

2.6 Cybersecurity Frameworks Applicable to the Space Industry

Several cybersecurity frameworks have been analysed to identify elements that can improve and inform broader cybersecurity knowledge and competencies. The National Institute of Standards and Technology (NIST) [2] Cybersecurity Framework provides a structured approach for managing cybersecurity risks across critical infrastructure sectors, emphasising identification, protection, detection, response, and recovery from cybersecurity incidents. The Cybersecurity and Infrastructure Security Agency (CISA) has issued targeted recommendations to strengthen cybersecurity for space system operators. Additionally, the SPACE-SHIELD framework [67], analogous to MITRE ATT&CK, catalogues adversary tactics and techniques specific to the space environment, particularly focusing on the space segment and communication links. NASA's Space Security Best practices Guide [68] outlines cybersecurity principles tailored specifically for space systems, supporting Space Policy Directive-5. Also, the Zero Trust Architecture for Space Systems emphasises strict verification and continuous monitoring, assuming threats exist both inside and outside network boundaries. Numerous studies highlight that effective space sector cybersecurity needs government collaboration and international cooperation to address evolving threats.

2.7 Training Needs Analysis (TNA)

TNA is a method of determining the need for training and what is required to address the knowledge or skills gap [69, 70]. The goal of a TNA is to determine the current state of education through surveys, interviews or secondary data [70]. The gap between the desired and current states represents the place for additional training [71, 70]. By providing the participants with the knowledge and skills they need, it is expected that their overall competency will be increased after the training [70]. The first step in a TNA is to identify the desired competencies required. This involves defining performance standards and job descriptions [72]. It is recommended to first determine whether current skills are lacking and if training is required before conducting a TNA [70]. The second step of a TNA focuses on determining key components such as identifying the target groups for training and selecting relevant interviewees who can provide valuable insights. This step involves selecting the appropriate data collection methods and creating a detailed survey plan [70]. Performing a gap analysis involves assessing the current performance or skill level of a department or employee, comparing it to a desired end state. This identifies the knowledge gap that needs to be addressed [73]. Although there are many different methods for conducting a gap analysis, the method for identifying the gap will usually depend on the organisation and the situation [73].
Gap analysis methods includes:

- Individual interviews: Interviews can be conducted individually with employees, managers and even with customers [73].
- Surveys questionnaires and self-assessments: Surveys are one of the data gathering methods designed to systematically gather quantitative information from individuals to gain insights into a larger population [74, 75]. Conducting a survey involves addressing various questions, such as determining the participants, formulating questions, and choosing a suitable data collection method [75]. Despite the simplicity of the concept, surveys can range from straightforward questionnaires to complex, multinational studies requiring multiple languages [75].

With numerous data collection options available, the challenge remains to produce precise assessments considering social, economic, and technological factors [75]. After determining the knowledge gaps, the next step in a TNA is prioritising the most critical gaps to identify training requirements [72]. Gaps can be analysed from the information gathered during the previous steps [72].

2.7.1 Creating Questionnaires

When creating questionnaires, it is important to take into account the format of the questions, content, wording, and arrangement. There are two different types of questioning that can be used: closed-ended questions and open-ended questions [70].
Closed-ended questions restrict respondents' answers. The respondents have the ability to select from a pre-established set of responses: (e.g., yes/no, "other" option, or response on a rating scale) [70]. The term "scale question" refers to the most typical type of ranking scale question. This type of question prompts respondents to consider a statement and then "rank" it based on how much they agree [70]. Closed-ended questions have several advantages, such as being easier and quicker to answer and thus easier to compare between respondents [76]. However, closed-ended questions may introduce bias by forcing respondents to select only from the available options, causing frustration. It may also be difficult to analyse how well the question was understood based on the answers given [76]. Depending on the survey, open-ended questions are written so that respondents are encouraged to answer the questions in the way they desire. This can be with a sentence, a paragraph, or a longer response. Instead of providing answers, respondents are given no options [70]. It is recommended to use open-ended questions only when really necessary, as more time is required both in answering the question and analysing the results [76]. Closed and open-ended questions can be combined in surveys. Closed-ended questions can be used to get respondents "warmed up", and then continue with open-ended questions [70].

2.7.2 Interviews

Interviews are one of the most direct methods of TNA data collection. By conducting interviews, in-depth data can be collected, allowing flexibility. For successful interviews, the planning phase must be done carefully. The planning phase includes the design of the questions, asking consistent questions, and determining a suitable way for conducting them. Using open-ended questions is important since not all questions can be answered with a yes/no. By conducting interviews, there is further freedom in introducing the purpose. For example: using a moderate tone, starting with questions that are easier to understand and do not veer into different topics, and categorising the questions. Lastly, show appreciation for respondents' participation [72].

2.7.3 Analysing the Data

Collected data most likely will not directly lead to the decisions. In the end, the most common and critical needs must be prioritised. Quantitative data formats can be analysed using graphs, tables, or charts. Qualitative data leave more to to analysis, but may provide valuable insights depending on the question [72].

2.8 The Space Industry in Estonia

As a global leader in digital innovation, Estonia has successfully integrated innovative technology into various sectors, including space and cybersecurity [77, 78]. Though the nation's contributions to space technology date back more than 70 years [79, 80], Estonia has solified its position as a space nation more recently with the launch of the ESTCube-1 satellite in 2013 [81]. Subsequently, Estonia became a full member of the European Space Agency in 2015, allowing its companies and researchers to participate in ESA projects and funding programmes [82]. Since then, Estonia has signed cooperation agreements with NASA and joined the Artemis Accords, strengthening its role in international space exploration [83].

Estonia's commitment to developing its space sector is further evidenced via plans to launch its first commercial satellite in early 2026 [84]. This initiative is a collaboration between Estonian companies and ESA, marking a significant milestone in space missions. Additionally, Estonian companies Spaceit OÜ and Golbriak Space OÜ, in partnership with Hungary's C3S LLC, are working under ESA's OPS-SAT ORIOLE project [85]. This collaboration aims to develop and launch an innovative optical communication satellite, further solidifying Estonia's role in the commercial space industry.

2.8.1 The Role of Cybersecurity in the Estonian Space Agency

As one of the most digitally advanced nations in the world, Estonia has prioritised space cybersecurity as a critical area of development [86, 87, 22]. More recently, the European Space Agency announced the establishment of Europe's space cybersecurity testing ground in Estonia, reinforcing the country's position as a leader in securing space assets [77]. This Space Cyber Range provides a dedicated environment for testing and enhancing cybersecurity measures for space technology [25]. Estonia's national space policy also emphasises cybersecurity as a key pillar of its space strategy [87].

2.8.2 Cybersecurity Frameworks in Estonia

In 2022, Estonia introduced mandatory cybersecurity requirements for systems critical to societal operations. A central aspect of these requirements is the implementation of information security standards, specifically the Estonian Information Security Standard (E-ITS) and the international ISO/IEC 27001 standard. The E-ITS, developed by Estonia's Information System Authority, aligns with both Estonian legislation and ISO/IEC 27001. Since its enforcement in December 2022, most obligated entities have begun adopting this standard [88].

The Estonian Information Security Standard (E-ITS) is designed to evaluate and certify the security of IT systems. E-ITS ensures compliance with international standards and provides methodologies for assessing vulnerabilities and implementing countermeasures, making it highly relevant for Estonia's critical infrastructure and digital systems [88].

3. Methodology

This chapter provided information about the methodology used to conduct this research study, largely guided by Cresswell (2018) [89]. Subsequently, methods for data gathering, analysis, and data visualisation are explained.

3.1 Justification

The research methodology focused on choosing methods most suitable for answering the research questions, aiming to gather optimum value in data. The pragmatic worldview was adopted as it allowed for the collection of diverse data, enabling broader analysis and reducing the risk of missing important insights [90]. A mixed methods research design was used, combining semi-structured interviews, surveys, and a review of relevant publications [89]. Qualitative and quantitative data were collected from surveys and semi-structured interviews. A convergent parallel mixed methods design [89] was selected, so that qualitative and quantitative data could be collected simultaneously for efficiency. Creswell [89, p. 48] explains truth in pragmatism as what works in a given context; truth is not based on a strict divide between objective reality and subjective perception. Truth is what works at that time. Thus, a mixed methods research draws on both quantitative and qualitative data, because combining them offers the most effective way to understand a complex research problem [89]. Quantitative methods may restrict responses, while qualitative research allows for a more flexible and exploratory analysis [89]. For this study, qualitative methods was used to capture in-depth data; which are sector-specific challenges, current cybersecurity practices, and cybersecurity training needs. Quantitative data was used to identify perceived cybersecurity knowledge levels to identify if there is a need for training, also comparing the results across different groups of questions. Thus, qualitative and quantitative data were analysed separately and then brought together to compare and better understand the answers provided, aiming to validate them by triangulation method [91, 92]. Results were also externally validated by experts. The selection of participants was justified by their direct involvement in space industry amongst diverse roles in Estonia, including cybersecurity professionals. This methodological approach and philosophy were chosen because they supported the exploration of practical outcomes, allowing conclusions to be drawn from multiple perspectives.

3.2 Research Design

A mixed-methods research approach with a pragmatic worldview was adopted. Both qualitative and quantitative methods were selected for data collection. Quantitative data collection method was selected for assessing perceived cybersecurity competency. Then, qualitative data were chosen to gather in-depth data, diving into a complex research problem, collecting data from various perspectives to see similarities in between the responses. Also, a mixed methods data collection allowed for a comparison in qualitative insights with the measurable patterns identified through quantitative data. A comprehensive literature review was conducted for examining existing current cybersecurity landscape in the space domain, including challenges, frameworks, and standards. Also, existing literature was used for forming interview questions and conducting a TNA. Multiple interview and TNA guides were used on the creation of both open-ended and closed ended questions [76, 70, 34]. Questions asked during the interview mapped into the research questions formulated [93]. The participants were determined via professional networks, and the questions were sent out before the interview, allowing them to prepare. Interviews were conducted virtually or in person, depending on the availability of the participant. Interview questions were validated by participants [93], giving their feedback. Quantitative data was collected from closed-ended survey responses and then was analysed to measure the perceived cybersecurity knowledge among professionals, compared results across different groups of questions. Thus, interview and survey data were analysed separately and brought together to compare, better understand the answers given and validate them by triangulation method [91, 92]. Then, results were validated externally by space cybersecurity experts to confirm the interpretations and conclusions were sound and validated internally using triangulation method [91, 89].

Table 4 presented the interview questions that were mapped to answer the formulated research questions guiding this study. The full list of questions is available in Appendix 2.

Table 4. Mapping of Research Questions to Corresponding Interview Questions

Research Question	**Questionnaire Items**
RQ1	Q1, Q2, Q3
RQ2	Q4, Q5, Q6, Q7, Q8, Q14, Q17, Q18
RQ3	Q15, Q16, Q22, Q24

3.3 Data Analysis

This section explains all the manual and statistical methods used to analyse the interview data and the technology used for data visualisation. Interviews were recorded with consent and transcribed. With the data acquired, both the quantitative and qualitative databases were displayed in JSON format. Interview data were stored in JSON files, each containing a list of question-answer pairs. Python's built-in JSON module was used to parse these files and extract responses. Textual responses were tokenised using the Natural Language Toolkit (NLTK) [94] library to split each response into individual word tokens. The RAKE (Rapid Automatic Keyword Extraction), algorithm was used to extract key themes from the aggregated textual responses. RAKE is an unsupervised, domain-independent algorithm designed to identify multiword phrases that are likely to be meaningful. In this study, the RAKE implementation from the RAKE-NLTK Python package was used [95]. For each sentence, the functions in RAKE package checked which of the top themes appeared. If two or more themes were presented in the same sentence, this was tagged as a co-occurrence. The spaCy package is a widely used Python library for Natural Language Processing (NLP) tasks, with the "en_core_web_sm" model; was used to segment the aggregated text into sentences to match RAKE-extracted themes within each sentence. The NetworkX package was used to construct and analyse the co-occurrence network. This approach, also helped to not miss any themes. Constructed graph nodes represented individual RAKE themes. Edges represent co-occurrence of themes within the same sentence. Themes were initially created by manual coding, using Delve software; SpaCy & RAKE packages was only used for cross-checking the themes that were found at the beginning, aiming to reduce bias. Also, Matplotlib & NetworkX packages was used for data visualisation purposes [96, 97]. For quantitative analysis, descriptive statistics had been used to measure central tendency calculating mean and median [98]. Yes/No questions used for making comparisons, forming correlations. The Pearson correlation matrix function from the pandas package was used to create the matrix, and the seaborn package was used to create the heatmap graph [99, 100].

Technology used including software, packages and data format for top phrase identification and data visualisation that helped data analysis were presented below, in the Table 5.

Table 5. Utilised Software and Packages for Data Summarisation and Visualisation

Technology	**Purpose/Usage**
Delve	Manual coding software
Python(3.9.6)	Chosen programming language
Jupyter Notebook	Interactive analysis and visualisation
JSON	Lightweight data storage format
NumPy	Numerical operations
Pandas	Data manipulation and and analysis (DataFrames)
Seaborn	Statistical plots
Matplotlib	General plotting
NLTK	Tokenisation, stemming, and corpus-level NLP
RAKE_NLTK	Key point extraction
SpaCy	Natural language processing package
NetworkX	Complex network manipulating package

3.4 Data Management and Ethical Considerations

Ethical considerations were addressed carefully, due to the sensitivity of the topic [101]. As some discussions may have involved sensitive topics, necessary measures were taken to ensure confidentiality and anonymity. Recorded data was transcribed manually, following Braun & Clarke method for getting familiarised with the data collected [102]. Consent was first obtained verbally and while recording during the video call, due to most of the interviews were conducted remotely. Then, consent forms were sent out for participants to acknowledge and sign. Signed consent was obtained from all participants, supporting voluntary participation and transparency in data collection. The study also adhered to academic and legal guidelines for handling sensitive information as the data was transcribed manually, and it has not been shared with a third party, only presented in the thesis, anonymised. Also, participants were asked for their preference of data presented in the participant table, asking for comfortability of their institutions and/or companies' names. As some of them might be obvious, and it could lead to identification of the participant. Company or institution names mentioned during the interviews that were censored as "[...]", for not exposing their perspectives. Also, findings did not expose specific vulnerabilities but rather contributed to the broader goal of strengthening cybersecurity awareness and training within the Estonian space industry. Full transcript has not been included in the appendix since it possibly could violate privacy, and only quoted qualitative data that was already presented in the study was included.

3.5 List of the Participants in the Study

Table 6 presented a listing of all participants involved in the study, detailing their respective roles, the number of years of experience, and the organisation they represent to provide a

clear overview of the individuals contributing to the research assuring anonymity. Participants were explained and been asked their preference of wording in the list regarding to their role and organisation for their comfortability with the data shared. Participants were listed as (P1, P2...) accordingly to their date of participation.

Table 6. List of Participants in the Study

Participant ID	**Role**	**Experience**	**Organisation**	**Interview Date**
P1	Chief Technology Officer (CTO)	11	Space Data Analytics Company	11-11-2024
P2	Founder	10	Seed-Stage Space SME	23-11-2024
P3	Project Manager	5	Cybersecurity Research Company	09-01-2025
P4	Coordinator	3	Public Sector	10-01-2025
P5	Research Assistant	1	Cybersecurity Research Company	16-01-2025
P6	System Engineer	7	Student Satellite organisation	17-01-2025
P7	Engineer	9	Tartu Observatory	27-01-2025
P8	Founder & CTO	15	Space Operations Company	30-01-2025
P9	Space Systems Engineer	10	Space Startup	05-02-2025
P10	Space Programme Security Accreditation Manager	5	International Space Agency	10-02-2025
P11	Head of Country Capability and Support Division	10	International Space Agency	04-04-2025
P12	Graduate Trainee	2	International Space Agency	04-04-2025

4. Analysis

This chapter presented the key findings of the analysis from the gathered quantitive and qualitative data. The first part of the analysis was descriptive statistics derived from the self assessment of perceived cybersecurity knowledge, yes/no survey questions, including a correlation matrix. The second part of the analysis presented the qualitative findings organised thematically based on patterns identified during manual coding, supported by key points extracted by Natural Language Processing (NLP) tools. Direct quotes are used to support the context behind these responses. These key points and co-occurrence graph of top themes are used for visual illustration.

4.1 RQ1: What is the Current State of Perceived Knowledge of Cybersecurity among Professionals in the Estonian Space Industry?

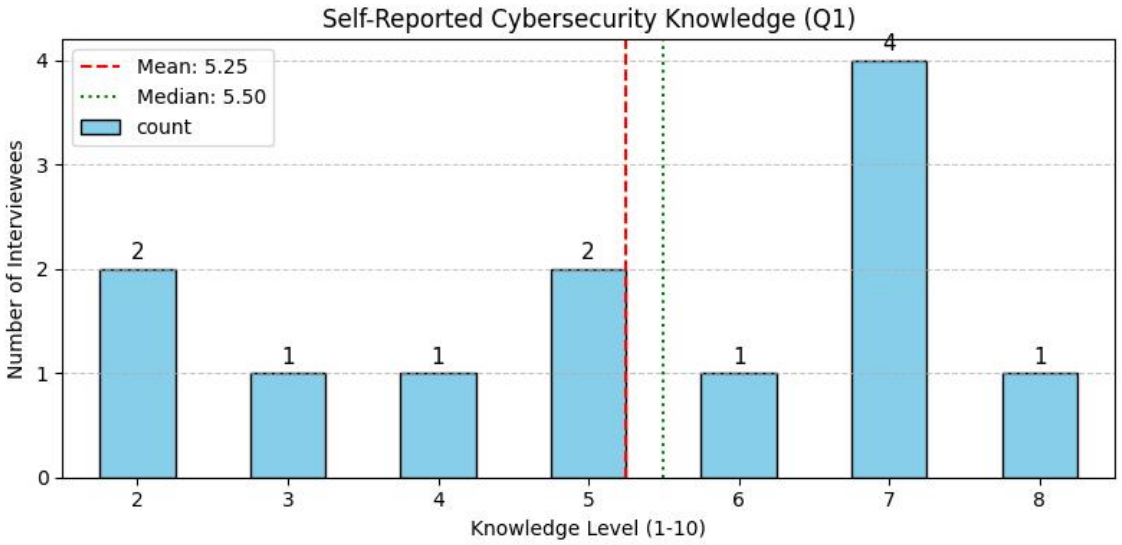

Figure 1. Perceived Cybersecurity Knowledge Levels

Figure 1 presents a bar chart illustrating self-reported cybersecurity knowledge of 12 interviewees on a scale from 1 to 10. The x-axis represents knowledge levels, while the y-axis indicates the number of participants at each level. The distribution shows that most participants rated themselves between levels 2 and 8, with the majority clustering around the mid-range (levels 4 to 7). Level 7 was the most frequently selected, with 4 participants' vote, while level 8, 6, 4, and 3 was the least frequently selected with one participants' vote for each level. The chart also includes visual markers for the mean (5.25, shown as a red dashed line) and the median (5.5, shown as a green dotted line), highlighting the central tendency of the responses.

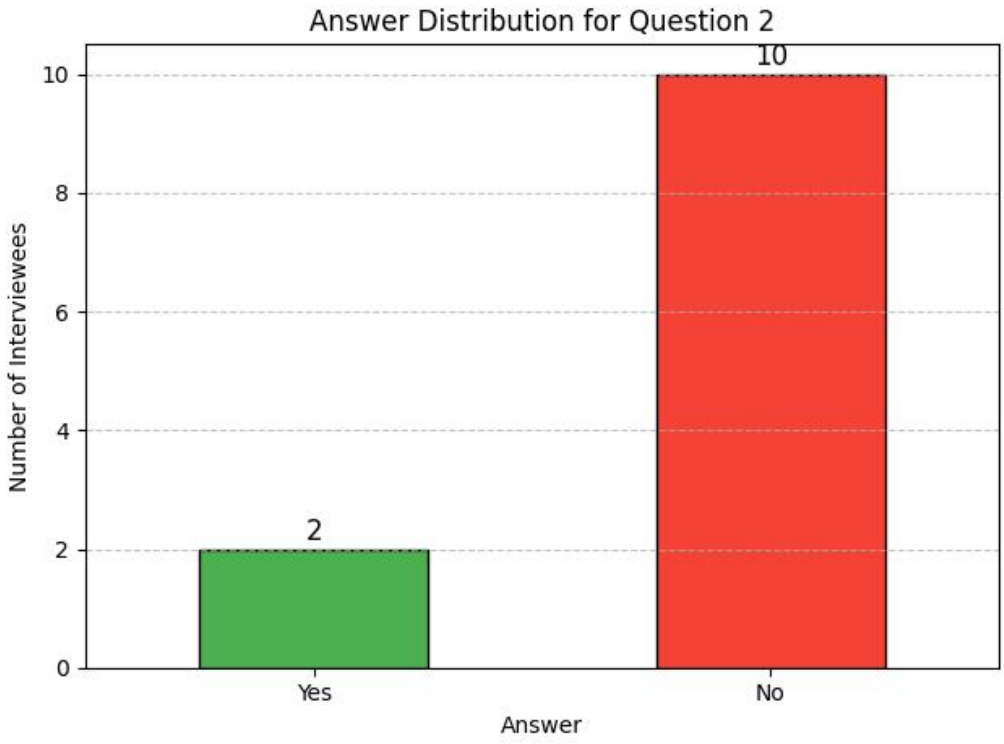

Figure 2. Distribution of Responses to the Question 2

Figure 2 represented the distribution of responses to Q2: "Have you received any formal cybersecurity training in the last 12 months?" Out of 12 participants, 2 received cybersecurity training, while 10 did not. Additionally, most participants answered "N/A" when asked if they had received any cybersecurity training. "N/A" was interpreted as a no.

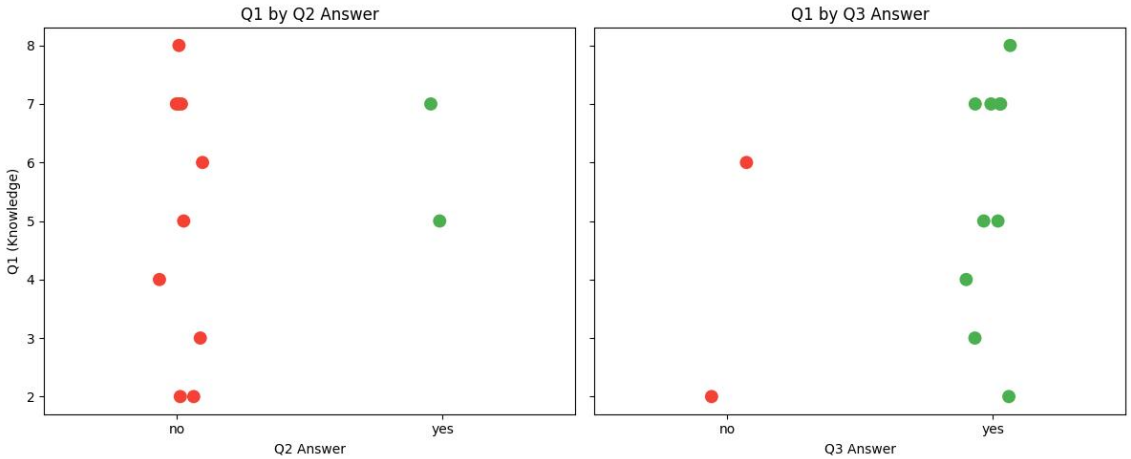

Figure 3. Relationship Between Knowledge Q1 and Responses to Q2 and Q3

These plots illustrated the association between participants' knowledge scores in Q1: "How would you rate your perceived knowledge of cybersecurity in the space industry on a scale from 1 to 10?", their responses to Q2: "Have you received any formal cybersecurity training in the last 12 months?" and to Q3: "Do you believe your current knowledge of cybersecurity

is adequate for your role?" Only 2 participants had received cybersecurity training in the past 12 months, with their self-assessed scores being 5 and 7. The self-assessed scores of the 10 participants who did not receive training show a regular distribution without clustering. The overall average score is 5.25, while the average score of those who received training is 6. In Q3: 8 participants who did not receive training stated that their knowledge is sufficient for their work.

4.2 RQ2: What are Current Cybersecurity practices among Professionals in the Estonian Space Industry?

To determine the current cybersecurity practice, 8 questions were asked: Q4, Q5, Q6, Q7, Q8, Q14, Q17, and Q18.

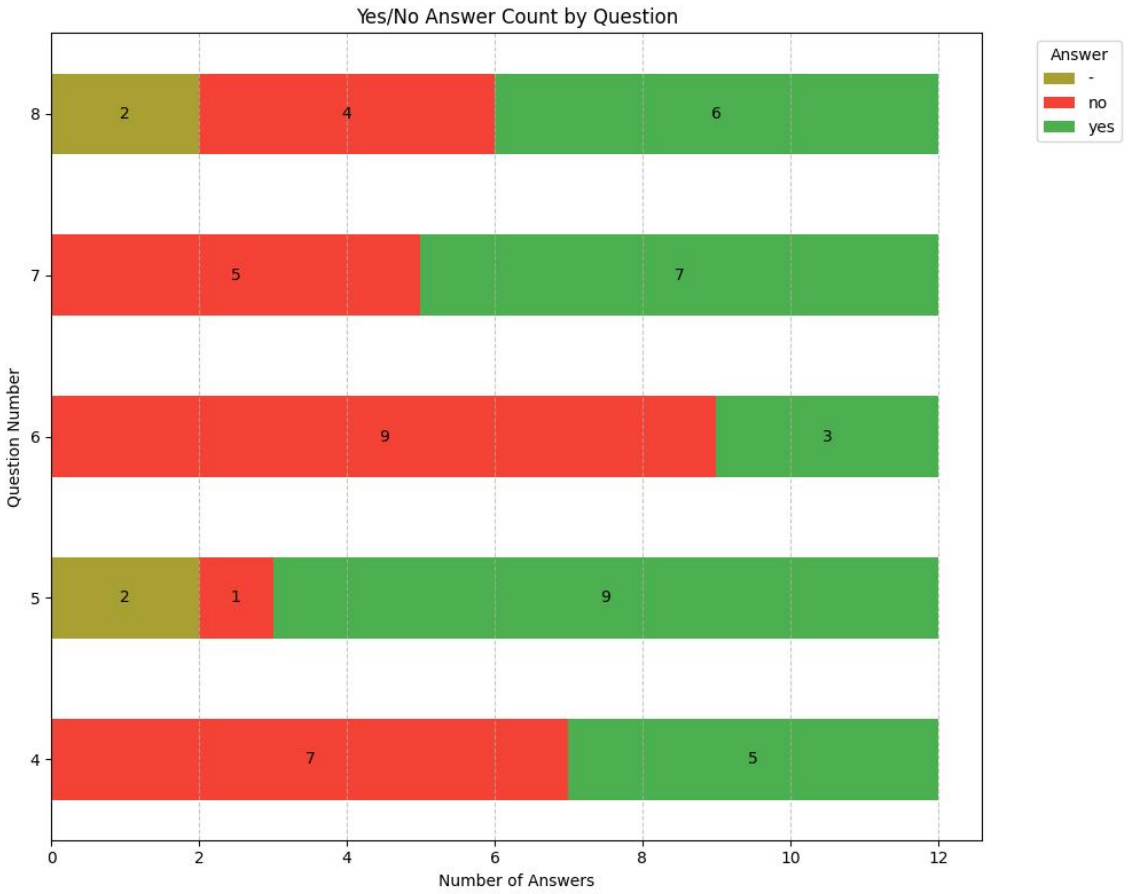

Figure 4. Distribution of Responses to Yes/No Questions for RQ2

Figure 4 presented the distribution of Yes/No responses to the questions posed in RQ2. For Q4: "Does your organisation have a dedicated cybersecurity team?", seven participants responded "No" while five indicated "Yes".
Regarding Q5: "Is cybersecurity considered a priority within your organisation?", the majority of participants answered "Yes", with only one participant responding "No" and

two choosing not to answer.

For Q6: "Is cybersecurity training mandatory in your organisation?", most participants answered "No" with only three reporting that mandatory training placed within their organisation.

In response to Q7: "Does your organisation perform regular security audits?", seven participants answered "Yes" while five indicated that they do not.

Finally, for Q8: "Do you feel that your organisation is adequately protected against cyber threats?", most participants responded "Yes", whereas four answered "No" and two did not answer.

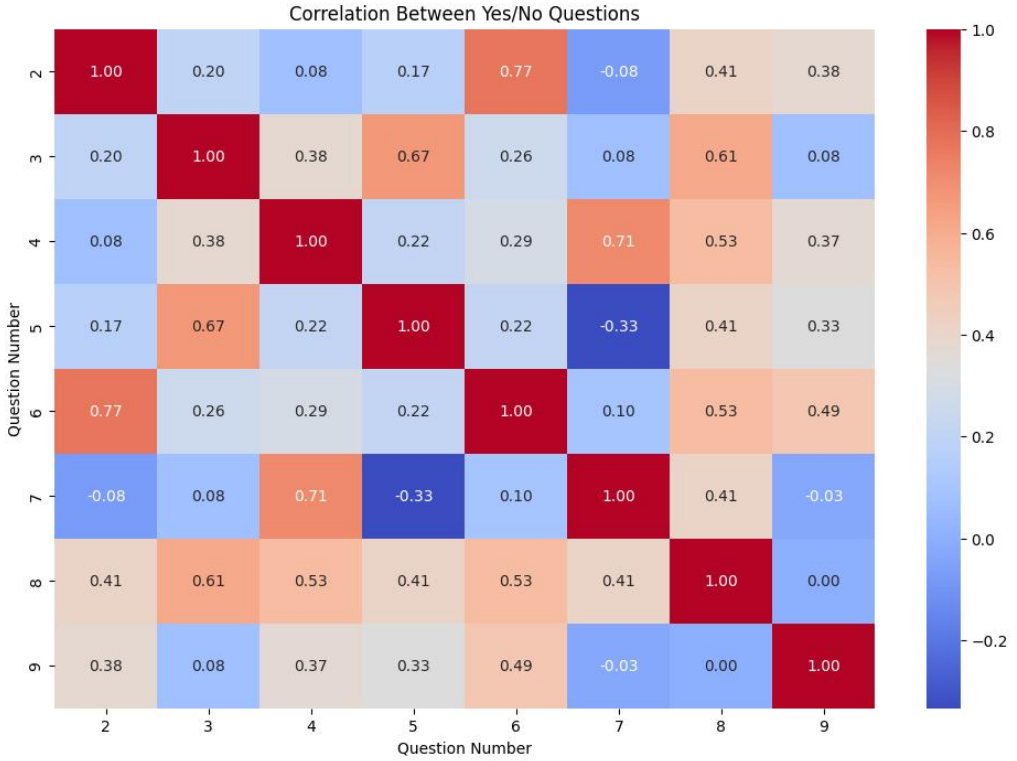

Figure 5. Correlation Between Yes/No Questions

Figure 5 is a heat map showing the correlation matrix between responses to yes/no questions, labelled by question numbers (2 to 9). The colour scale ranges from blue (negative correlation) to red (positive correlation), with the correlation values displayed in each cell. The highest correlation is between questions 2 and 6 (0.77), and between questions 4 and 7 (0.71). There are some negative correlations, such as between questions 5 and 7 (-0.33). Most correlations are positive, suggesting that responses to these questions tend to move together. Positive and negative correlations examined in detail below. Starting from the highest correlation question group (Q2 and Q6), and then highest negative correlation question group (Q5 and Q7) were examined.

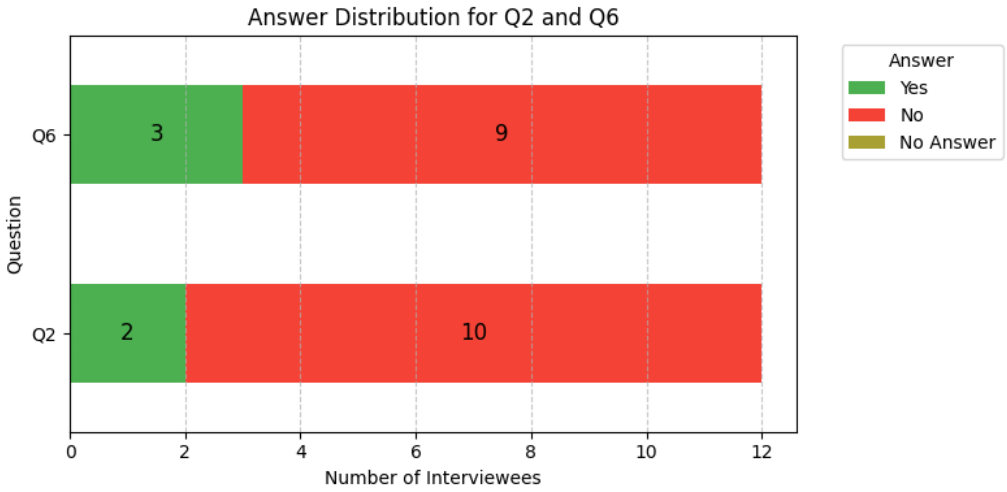

Figure 6. Comparison of Q2-Q6

Figure 6, represents the highest correlation spotted in the Yes/No questions, regarding to the question group (Q2: "Have you received any formal cybersecurity training in the last 12 months?" and Q6:"Is cybersecurity training mandatory in your organisation?"). While 9 participants consistently responded "No" to both questions, 2 participants answered "Yes" to both. One case stands out where an interviewee reported mandatory training at their organisation but had not received training in the past year.

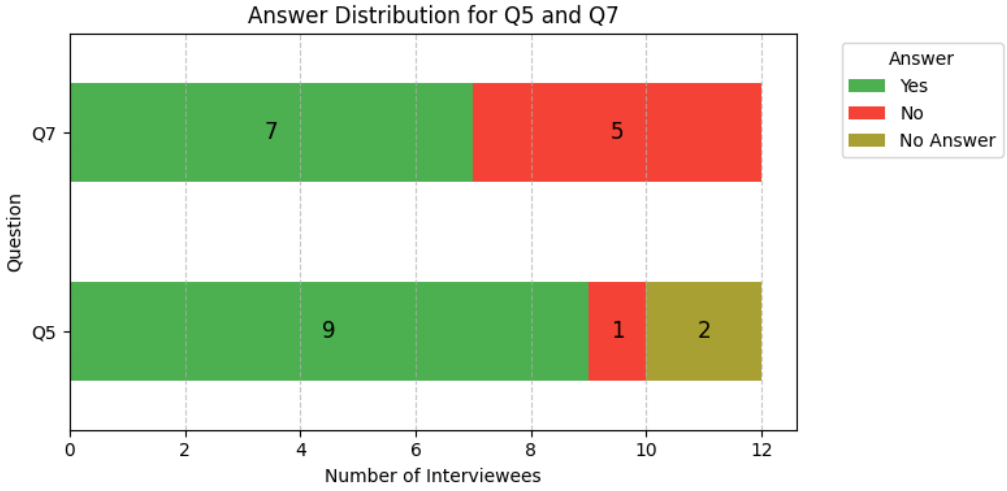

Figure 7. Comparison of Q5-Q7

Figure 7 illustrated the highest negative correlation spotted for the question group (Q5: "Is cybersecurity considered a priority in your organisation?" and Q7: "Does your organisation perform regular security audits"), the majority (9) answered "Yes," with only 1 "No" and 2 providing no answer. In contrast, Q7 had a more divided outcome, with 7 interviewees responding "Yes" and 5 responding "No". While this graph shows slightly negative correlation(-0.33), it additionally shows inconsistency, between recognising cybersecurity as a priority and conducting regular security audits.

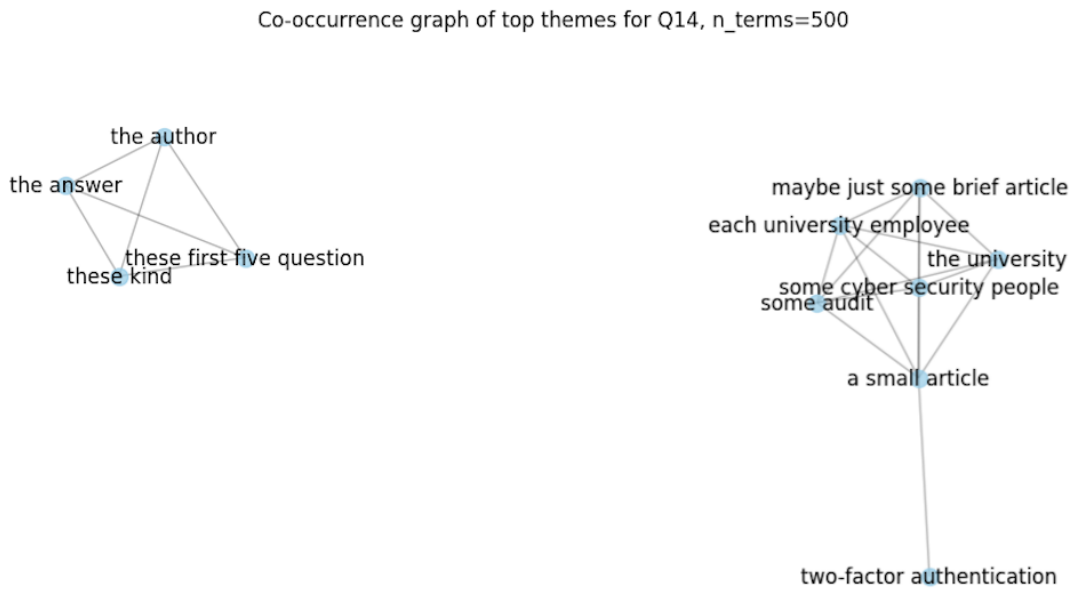

Figure 8. Co-occurrence Graph for Q14

Figure 8 illustrated the co-occurrence graph for relationships between terms in the text. When terms frequently co-occur, it suggests they are related or connected in meaning or theme. For Q14: "What type of cybersecurity training, if any, have you received?" While most of the participants answered "N/A", the top phrases identified were: "a small article, maybe just some brief article, university, some cybersecurity people, some audit, two-factor authentication". The identified phrases are introduced by quoting them as follows:

P4: "[...] was the author of that, so it is more like they ask these first five questions, it is these kinds of questions that you definitely don't know the answers to. They prove that you don't know anything about cybersecurity. This is what we're doing almost every year. It is very basic training that covers phishing and that."

P5: "A small course that is online, based on answering a questionnaire."

P6: "Thinking back, and maybe just some brief article that each university employee has to read - do not do this, try to not do that, and that's pretty much it. When I was in the [...] I remember getting some, I don't know, some cybersecurity people were doing some audits, and we just had a small article. I think it was a small article about how to set up two-factor authentication."

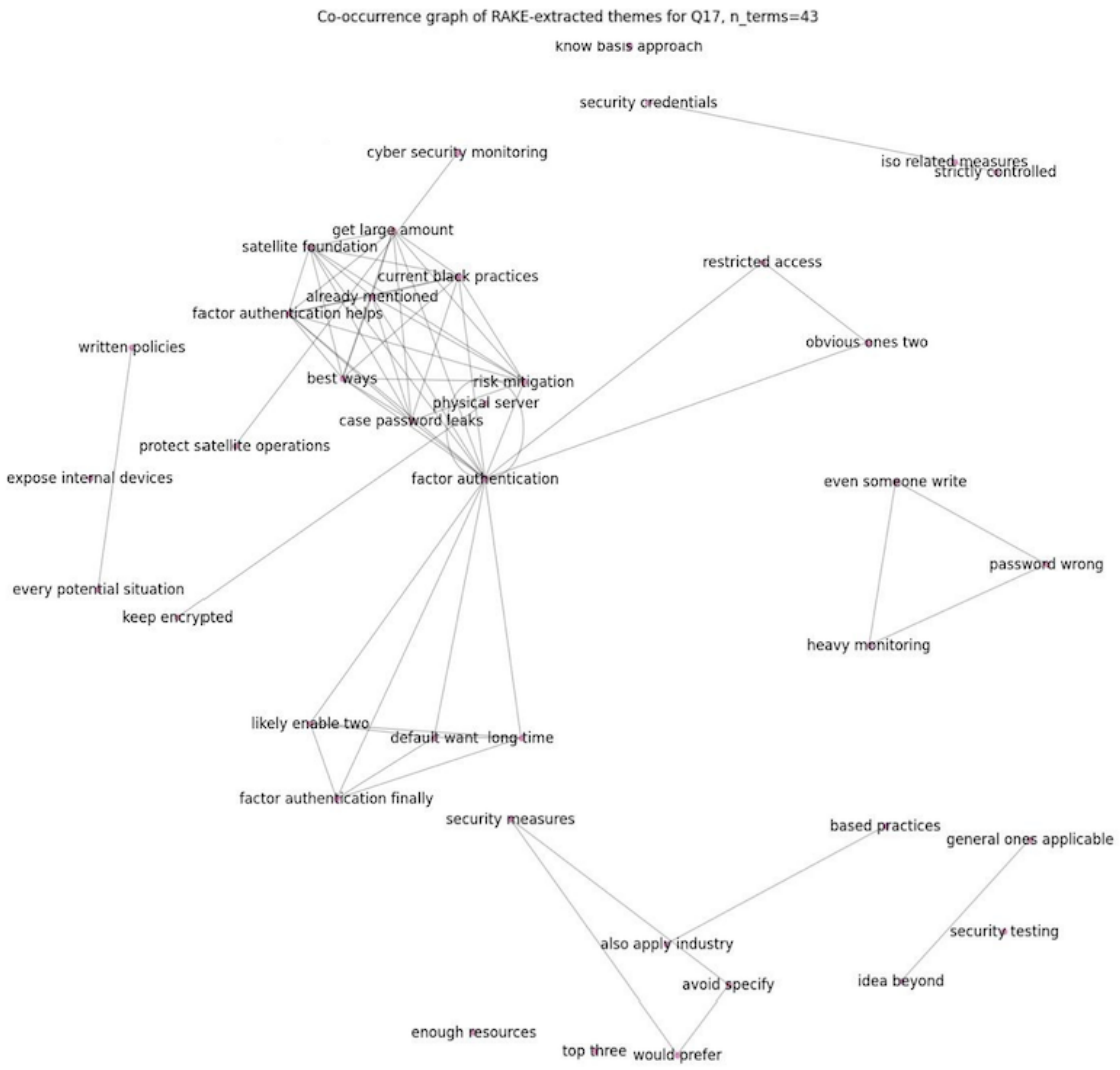

Figure 9. Co-occurrence Graph for Q17

Figure 9 represents a co-occurrence graph for the key points identified by NLP for Q17: "What cybersecurity measures are currently in place in your organisation?" Key points for the Q17 identified as: "the two-factor authentication, heavy monitoring, the general one, obvious ones, the space specific one, internal device, every potential situation". While two of the participants answered that they did not know, all of the answers from the participants provided an answer presented below:

P1: "There are silos, regular reviews and updates, and heavy monitoring. Even if someone enters their password incorrectly, it will be investigated."

P2: "We use internal VPNs, with all traffic tunnelled. We do not expose internal devices to the outside, and we employ encryption. We also maintain a physical server, which is kept encrypted, as well as regular back-ups."

P3: "ISO related measures"

P4: "I don’t know"

P5: "Quite the obvious ones: two-factor authentication, the restricted access to documents and to the premises, as well as infrastructure. The need-to-know basis approach to projects and documentation. Then, the trainings we have. These are probably the top three that come to mind."

P6: "We update our servers when we can and we are now going to most likely enable two-factor authentication finally for everyone, so it is something that we have thought about for a long time. To have it activated, then it is just time to make the switch and it is going to be a bit of a hassle, but I guess it is a good thing to do."

P7: "I think there isn’t really a risk mitigation like a campaign in that kind of in the [...] So, current practices as I already mentioned about the two-factor authentication seem to be one of the best ways to get a large amount of people to have more security against password leaks. Then at least the two-factor authentication helps it a bit, so that seems to work."

P8: "We do security testing. We match our security credentials, or let’s say they are strictly controlled. We also apply industry-based practices where possible while developing our services. We do not have written policies for every potential situation. Not enough resources for us."

P10: "Several, from cyber security monitoring to cryptography to protect satellite operations. I would prefer to avoid specifying too much because of the nature of our security measures."

P11: "I do not know"

P12: "I have no idea beyond the general ones applicable to all. I don’t know of the space-specific ones that are related to our industry."

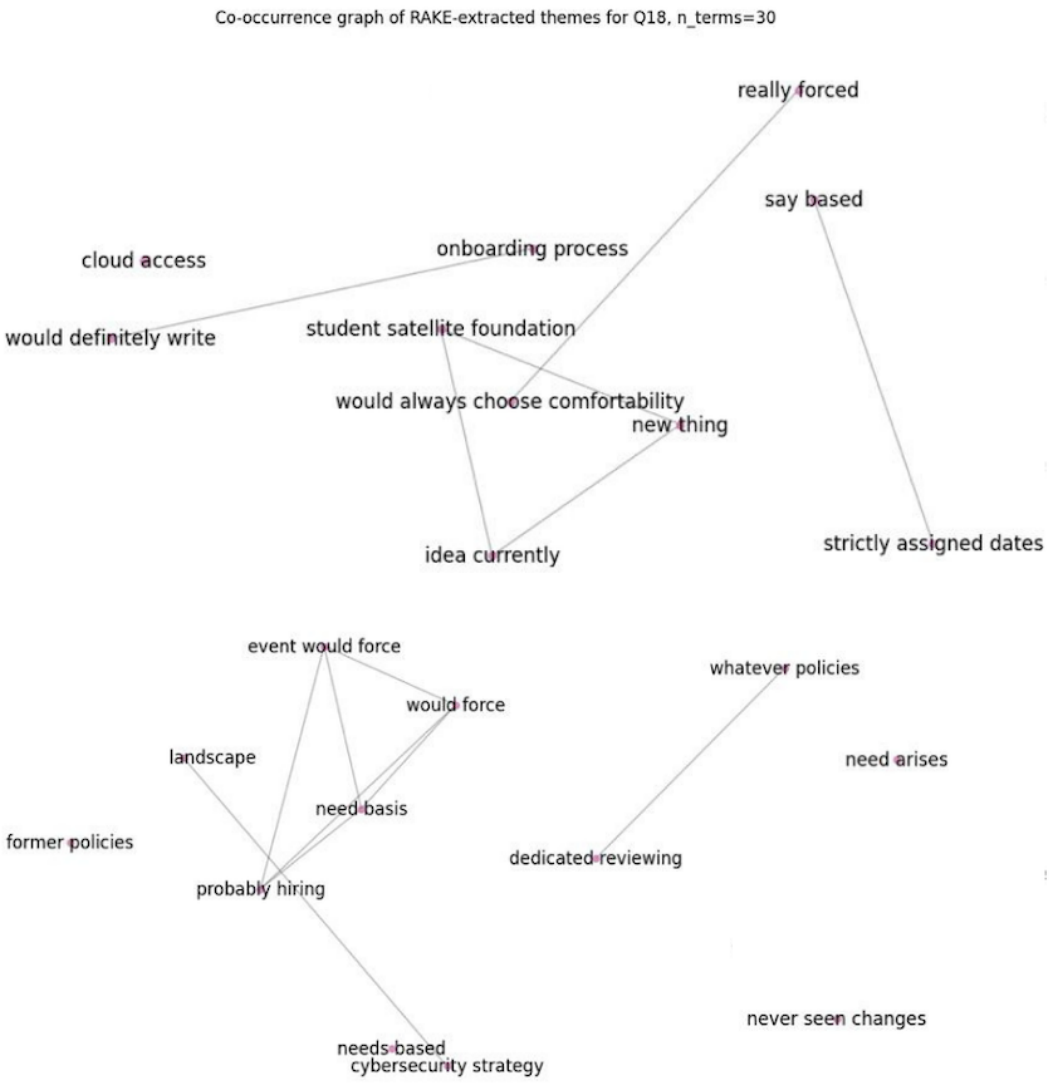

Figure 10. Co-occurrence Graph for Q18

Figure 10 below represents key points for Q18: "How often does your organisation review or update these policies?". NLP identified the top key points from responses to Q18 as "former policies, a need basis."

P1: "It's the kind of thing that we do continuously. We do not have a specific process. Whenever we feel like a change is needed."

P2: "We do not have former policies."

P3: "Yearly."

P4: "I've never seen changes in policy. Maybe once in 3 years. It is based on needs -there is no regularity."

P6: "We do not really do it - we just update it when the need arises. We don't really have a schedule. We do it when we have to, I guess. But we are not following industry best practices like every year. Now we have a dedicated reviewing of whatever policies we don't do that for."

P7: "I do not know about policies. This is a new thing about like reviews and policies of cyber securities. I have no idea currently. We do not really have reviews in the [...], and we don't have really a policy. Yeah, there should be a policy for you to read or update them."

P9: "We would definitely write down something - it is an onboarding process. Reviewing them, I think there must be some kind of event to force the review. So maybe, some data is stolen or maybe someone is actually hacked. So I think that kind of event would force the review of those policies, probably hiring a dedicated IT person, would force the review, but in generally, I don't think there would be anything regular, more like a need basis."

P10: "Regularly, based to the evolution of the threat landscape and our cybersecurity strategy."

4.3 RQ3: Which Training Measures Can Be Implemented to Improve the Cybersecurity Knowledge of Those Working in the Space Sector in Estonia?

To answer this research question, three questions were asked, mapping to questions 15, 22, and 24. Q15: "What are some of the main cybersecurity challenges you think the industry faces?". Then, in Q22: "In what areas do you think additional training or resources are needed for cybersecurity in your industry?" Lastly, Q24: "Are there any specific topics or issues you believe should be prioritised in future cybersecurity courses?" Themes were identified by manual coding. Then, NLP extraction was done to not miss any points that were made.

Key themes identified for Q15: "What are some of the main cybersecurity challenges you think the industry faces?", during manual coding: "Cybersecurity unawareness", "Geopolitical situations", and "Legacy systems". Figure 11 represents the visual image of the responses provided to Q15.

Figure 11. Word Cloud for Q15

Theme 1: "Cybersecurity Unawareness"

P2: "I think most of the time people neglect cybersecurity. At least in the CubeSAT area where we are more familiar. I think it becomes important only when something bad happens. You know better than I do, hundreds of CVE's. So I think that's really the issue."

P4: "Definitely, there is a heavy underestimation. At first people, were laughing at it like this is not an issue why are you putting your energy on this? And then, in 2022 the world was proved that everyone was shown through the viasat satellite hack before the invasion of Ukraine. This is an issue and the space sector has heavy vulnerabilities in space that our space objects are not cyber secure and this is a very underestimated security issue that we have. The main challenge so far is that most spacecrafts on orbit today are not cybersecure."

P10: "The space sector is one of the last industrial domain where cybersecurity is being introduced. Therefore, the key risk is that the industrial ecosystem is not fully ready in managing overall security incidents, from the identification up to the response and recovery measures. This include not only their corporate activities, but also the security of the space assets once in operations. One further point that is critical is the management of the supply chain, which may pose serious risks to space assets and missions."

Theme 2: "Geopolitical Situation and Actors"

P1: "Well, I can't get around Russia at the moment due to the war in Ukraine. The efforts

that are being undertaken are so much less subtle and so much more direct. Basically every part of the system is vulnerable in some way. I think they're using all of the methods. So anything from tapping undersea cables to having students go through bachelors masters and doctorate programmes that end up in the industries, people, education, good job tech and then leverage using their family or parents at home to provide information on these companies and agencies. I definitely think that is inside vector. Satellites - You can't even upgrade or retract, so we're going to have a bunch of satellites up there, but they are going to become vulnerable in the next 10 years that we cannot upgrade. Some of the techniques that had been used on smaller scales, but they are pretty troubling. Various jamming techniques so that will be there was a multi month period, where we can land planes using GPS in Finland and I think near here as well, because the Russians were jamming the cheapest frequencies that can cause massive massive outages in various sectors. Basically anything with automatic navigation that we used. It all depends on the GPS, now all the new cars they are all dependent. So you can just buy denial of service for hours or days or even even weeks you can crash subsections of the economy. We have old satellites up there that have no security and they're mostly out of fuel. What you can also do is, even if you don't cause any damage, if you don't destroy it, you can de-orbit it. I don't know that's kind of hopeless issue. I look at it from the perspective, I'm looking at it from an attackers perspective."
P5: "Since the situation in Europe and in different places in the world currently is quite unstable, then we are not sure what kind of actors and what kind of attacks will be put against the systems that we have."
P9: "All those software-defined radios, many old space systems against actors. US, Europe against Russia and China, they really seem to be wanting to do bad things. Actually trying to harm cables under seas, satellites also - with bad actors, definitely."

Theme 3: "Legacy Systems"
P2: "In software science, it's more generic, they tend to with this approach sort that works for hardware, so once it works, you don't change it. I think they also apply the same concept to the software. I think, sometimes on purpose even if they know they do not solve it because then it has to go back to the certification. We had to fight a lot, also for our system in the past."

P5: "I would definitely name the legacy systems that many organisations rely on. Since many satellites have been deployed a long time ago, and the security protocols and information that have been added to those satellites are based on previous knowledge, not the current knowledge. Then, legacy systems pose major threats. And also, challenges are in the increasing level of attacks that can be made from different actors. And the general geopolitical environment since the situation in Europe and in different places in the world

currently is quite unstable, then we are not sure what kind of actors and what kind of attacks will be put against the systems that we have."

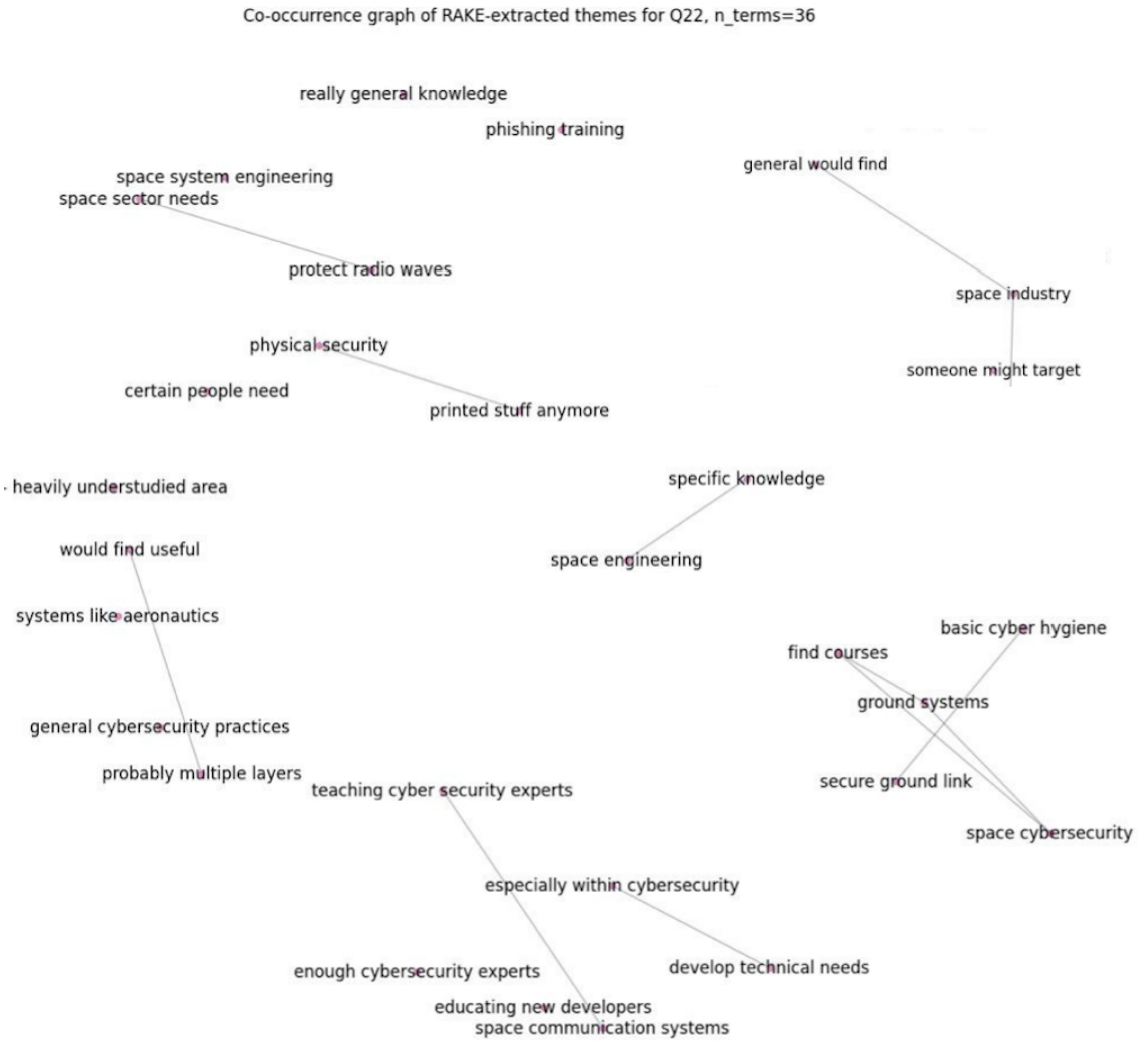

Figure 12. Co-occurrence Graph for Q22

Figure 12, represented co-occurrence graph for Q22. Q22: "In what areas do you think additional training or resources are needed for cybersecurity in your industry?". During manual coding, based on the answers participants have provided, two themes identified: "Industry Wide Need Expertise" and "Cybersecurity Awareness"

4 of the participants agreed upon that there is a need for industry wide need expertise. Theme 1: "Industry Wide Need Expertise"

P4: "Definitely, the space particularities and interdependencies. heavily understudied area, especially in Europe. We don't have enough cybersecurity experts in the field of space. No cybersecurity experts teaching space communication systems. so teaching cyber security experts the particularities of space and space communication systems and studying how to detect hacking is very important."

P5: "We can see that there is a need for space related projects and developments, especially within cybersecurity, then the knowledge that is required to be able to develop technical needs and trainings for cyber range is lacking. I would say that resources are limited and people available are also limited. And educating new developers to be knowledgeable in this field is beneficial, as well as for myself. And I believe learning about space and specific technological questions that are related to that is needed. I am planning myself to find courses or educate myself in any possible way on both space cybersecurity and as well the technical aspects of satellites and ground systems."

P8: "So, educate people to understand what is happening and how to protect themselves and the industry as such. Then, of course, certain people need more exposure to the specifics as well."

P10: "More in general, it is missing a job figure that mixes expertise on both cyber and space system engineering."

Theme 2: "Cybersecurity Awareness"
P8: "I think the overall level of cybersecurity must be raised, as in other industries as well."

P12: "I think there's probably multiple layers of training that they would find useful. One just awareness of the different ways, that a cyber attack could look like and different types of cyber attack."

Also one of the participants mentioned the necessity of regular cybersecurity training:
P7: "The regular training should be mandatory because whatever I did in bachelors I have already forgotten regarding most of the infrastructure access for example how to do SSH properly and all these things we kind of do it with some simple way but well I think it's important to have once in a year or at least once a year every two years some kind of a training that would keep everyone on the same page, like what you should do, what you shouldn't do, how to do it properly and all that."

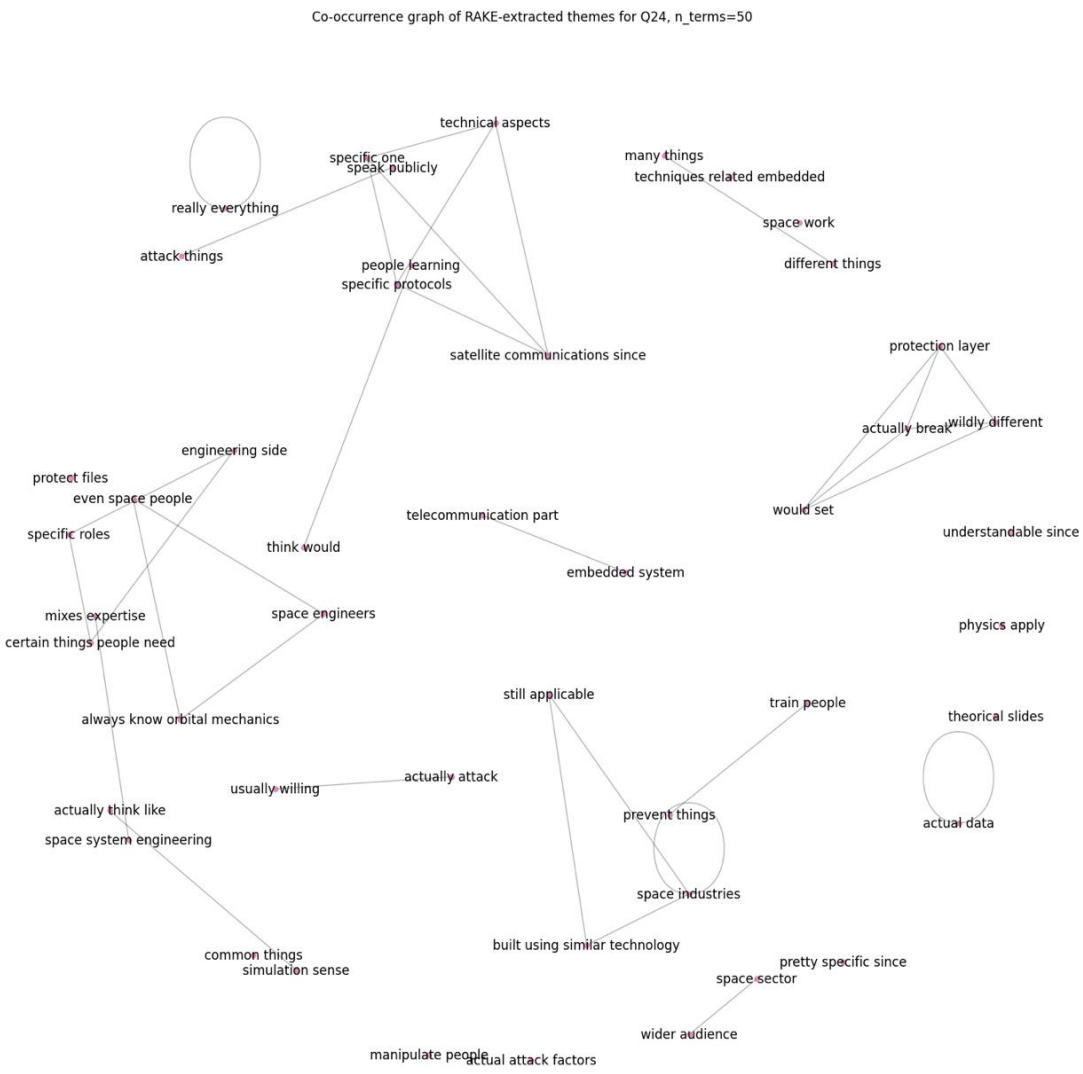

Figure 13. Co-occurrence Graph for Q24

While the top themes are identified by NLP are presented in the Figure 13, answers to Q24: "Are there any specific topics or issues you believe should be prioritised in future cybersecurity courses?" identified by manual coding were: "Industry Specific Knowledge", "General Cybersecurity Knowledge and Basic Cyber Hygiene", "Practical Applications", "Attackers Perspective", and "An Introductory Course".

Theme 1: "General Cybersecurity Knowledge and Basic Cyber Hygiene"
4 of the participants agreed upon the importance of basics of the cybersecurity knowledge.

P2: "General security, file management, to whom you share, document, digital signature. To protect files and so on."

P6: "I think it all starts with basic cyber hygiene. Try to not reuse passwords and secure

ground link or ground stations. I don't really think there is anything super specific that we need to do regarding satellites."

P8: "It depends on the audience. If you take a wider audience from the space sector, it's basics. Or basically, it has huge impact, I think."

P11: "I suspect that the technologies and techniques involved are not widely known or understood outside specialist circles. Across the entire space industry, I do not think this knowledge is widespread. It seems to me that it remains highly specialised, with only certain individuals within companies or organisations possessing the necessary expertise and dealing with these matters. It is not really a general knowledge."

Theme 2: "Industry-Specific Knowledge"
4 of the participants agreed that industry specific knowledge is needed.

P3: "Industry-specific knowledge about space engineering"

P5: "Currently, the cybersecurity courses are more generic, which is understandable since the industry works this way. But for satellites, the knowledge has to be pretty specific since the vulnerabilities that are applied to satellites are different from the generic ones. More specialised. It can be specific protocols that can be vulnerable to attacks or just the general knowledge of what kind of systems are the weakest in the satellites and what kind of advantages can be in protecting those systems as well as, what I'm saying, the technical aspects of both ground and satellite communications since these are, not the most generic knowledge, but a very specific one"

P7: "What was lacking that people didn't know what is space, how does space work and I think that was quite a thing that is needed, that sort of education is needed and even space people, space engineers, not always know the orbital mechanics."

P10: "Cybersecurity aspects of spacecraft and On-board computers"

Theme 3: "Attackers Perspective"
P1: "We focus so much on how do we train people to prevent things, but we don't give the attacker's perspective. And that's for a few reasons. One of the reasons is none of the people who actually attack these things are usually willing to speak. They don't want to speak publicly, but we do have a few of them who used to attack things."

P7: "How do you understand and and how to what are the most common things that you

can do as a hacker? How to attack it because, well, from the point of cyber security if it's computers, you know, ground stations run on computers, therefore, the procedures are the same."

Theme 4: "Practical Applications"
P7: "I think the main point is to do the do the training that simulates an actual reality so so try to do as practical as possible so then uh then it's more clear how to do it and then if it's like something that [...] does with Cyber Range then you can create different kinds of scenarios which then can be like used as a way how to train people because in in any shape or form, if the event happens then the more training you have had, the less problems with understanding and less stress and/or feeling of unknown there is in general."

P9: "it would have to be very practical and pragmatic. If you say we need more defence, that doesn't do anything for me, hypothetical scenarios of hacking a satellite doesn't do anything for me, because, i think i have a better understanding how hard it is in practice. so you have to engage me, it would have to be realistic in other words.Just theoretical slides of hypothetical scenarios, it's very easy to dismiss in my psychology."

P12: "As I mentioned with an overview, something on protecting, actual data and images. Something on protecting the data centres and data access."

Theme 5: "An Introductory Course"
2 of the participants agreed upon an introductory course of the basics covering both cybersecurity and space is needed.

P7: "How can you build an orbit, and what are the parameters and what does it mean for the satellite to be visible only once in one and a half hours and all these sorts of things that should be just explained, and it shouldn't be too hard, well it's an introductory course."

P12: "Really everything. An introduction course."

Also, P4 suggested legal aspects of cybersecurity: "Hacking and threats. To focus on insurance, technicalities are very important, but also it's important to know the legal implications."

4.4 Future Expectations

All of the participants recognised that cybersecurity will become more critical in the space domain in the next 5 years. Theme "Leading Role" was identified.

Leading Role:
P4: "We foresee that Estonia should take a leading role in the field of teaching cybersecurity experts in Estonia. Today we are already ahead of most European countries so I think we should really use the momentum."
P7: "In principle we should push for the Estonia being the cybersecurity for space centre. So then there is a possibility to involve external parties or attract more people that could build the cybersecurity like sphere in Estonia in that sense."
P10: "Considering the relevance and expertise within the cybersecurity sector of the Estonian industries, it could be a leading and pioneering role."

Also, other participants added:
P1: "I think it is key, we should focus more on the security of satellites and systems and how it is evolving, I think it is interesting in Estonia because they're focusing a lot on it even though the space industry is quite small because it's passed another couple of companies."

P5: "Hopefully, it will be a growing sector for Estonia since we are relatively strong in IT systems and this is an industry that is still growing. There is expected to be a lot of new attacks as well as new possibilities for securing and protecting the systems. Estonia has definitely a huge opportunity in creating specialised courses. For example, in [...] or in [...], the cybersecurity courses can be modified to address specific satellite issues or ground system issues as well as creating some kind of either protocols or generalised systems that can frameworks, that can be applied to general European security or even global security."

P6: "Things are becoming more and more plug-and-play. So you are going to have more and more of these common central parts that everybody hooks their camera or a sensor to. So if you have like one satellite brain that is built in a very specific way and then you have another satellite brain built in another specific way. But if you have 100 brains that are identical and this has a camera and this has a death laser, then, I mean, it's very tempting to hack that specific satellite brain."

P7: "That are active and operating. Other universities throughout Europe starts cooperating with you and sending students to Estonia to learn missing part of the engineering while doing their course."

5. Discussion

This chapter discusses the interpretations of the findings presented in Chapter 4, addressing each research question in detail.

5.1 Current State of Cybersecurity Knowledge (RQ1)

The analysis revealed that cybersecurity knowledge among Estonian space industry professionals varies significantly. Most participants rated their knowledge as moderate (mean is calculated as 5.25 and median is 5.50) as illustrated in Figure 1. This indicates a general awareness of cybersecurity, but also indicates a lack of deep, specialised knowledge. Also, only CTOs and cybersecurity professionals graded their cybersecurity knowledge level high. The majority of other professionals rated their knowledge as moderate or low. Additionally, professionals believe there is a lack of expertise at the intersection of aerospace, computer engineering within industry and government workforces [63, 53]. The lack of formal cybersecurity training among most participants and the space industry professionals overall underscores this gap further. Professionals rely on self-learning and informal methods, which is invaluable, but may be insufficient in addressing the complex cybersecurity threats specific to the space sector.

Figure 3, illustrated the comparison of the answers given to Q1 (cybersecurity knowledge), Q2 (cybersecurity training), and Q3 (regular audits). Participants who received training (scores 5 and 7) rated themselves slightly higher than the overall average (5.25). Although this suggests training may positively influence self-perceived cybersecurity knowledge, the small sample size (only 2 trained participants) limits the strength of this conclusion.

5.2 Current Cybersecurity Practices (RQ2)

The analysis identified several shortcomings in current cybersecurity practices. Although some companies indicated continuous and proactive cybersecurity approach, some professionals indicated rather a reactive approach, implementing security measures only after experiencing incidents or facing regulatory pressures. This reactive approach is insufficient given the critical nature of space infrastructure and the potential consequences of cyber incidents [50].

The lack of dedicated cybersecurity teams, particularly in smaller companies and projects

affiliated by universities, increases the potential risks. Without a personnel responsible for cybersecurity, organisations struggle to maintain consistent security practices and update policies actively. Also, inconsistent security policies and reliance on general university IT infrastructure for cybersecurity protection in academic projects indicate a significant gap in tailored cybersecurity measures. This inconsistency places such institutions vulnerable to cyber threats in danger of experiencing data leaks.

The data presented in Figure 6 and 7 reveals a notable gap between organisational cybersecurity policies and their practical implementation. Specifically, Figure 6 demonstrates a clear positive correlation between mandatory cybersecurity training and actual training received, indicating that mandatory policies generally lead to higher compliance; however, the presence of an exception (where training was mandatory but not received) suggests potential issues in policy enforcement or communication. Conversely, Figure 7 shows a slight negative correlation and inconsistency between cybersecurity being recognised as a priority and the actual practice of conducting regular security audits. Although most participants acknowledge cybersecurity as important, fewer organisations consistently perform regular audits, indicating a disconnect between stated priorities and operational realities. Overall, these findings suggest that while organisations may formally recognise the importance of cybersecurity and develop relevant policies, there remains a significant challenge in effectively translating these policies into consistent, practical actions.

One of the participants noted that cybersecurity training must be mandatory, and another participant added that there must be an event forcing them to review these policies. This finding clearly shows the reliance on external parties, because organisations often wait until compelled by regulatory requirements to reassess their cybersecurity posture. This finding is supported by the results of the similar studies, stressing governments' and policymakers' involvement is necessary [52, 38].

To address these shortcomings, organisations must transition from reactive to proactive cybersecurity strategies. Having a dedicated cybersecurity team, even within smaller organisations and academic institutions, is essential for maintaining security practices, conducting regular audits, and updating policies. Additionally, cybersecurity should be integrated into the design phase, especially for space infrastructure projects [50, 51].

5.3 Cybersecurity Training Needs (RQ3)

The RQ3 is aimed to identify specific topics that should be prioritised in future cybersecurity courses within the space industry. The thematic analysis of participant responses revealed several key insights, identifying training needs.

5.3.1 General Cybersecurity and Basic Cyber Hygiene

Participants agreed upon the importance of foundational cybersecurity knowledge and basic cyber hygiene practices. Participants noted that general cybersecurity principles applicable to non-space industries remain highly relevant to the space sector, given the similarity in technologies. This finding suggests that future cybersecurity courses should continue to reinforce foundational cybersecurity practices regardless of the background. This approach supports best practices recommended by cybersecurity frameworks and standards, such as the NIST Cybersecurity Framework and ISO/IEC 27001, which emphasise the importance of basic cyber hygiene as a critical first line of defence against cyber threats [2, 1, 103].

5.3.2 Industry-Specific Cybersecurity Needs

Another finding from this study was the clear identification of a gap in the content of cybersecurity education. Participants agreed that industry-specific knowledge should be prioritised. Also, participants mentioned that satellite systems have unique vulnerabilities and operational environments that differ from generic cybersecurity contexts. The development of targeted space systems for cybersecurity curricula would significantly improve the cybersecurity preparedness within the space sector, supporting the findings from a similar study, particularly the industry professionals' perspective report [63, 53].

5.3.3 Practical Training and Applications

Another key finding from this study emphasised practical training and realistic simulations. The participants expressed the importance of practical applications, finding theoretical knowledge dismissible. This finding supports the importance and effectiveness of experiential learning approaches, such as cyber range exercises and scenario-based training. Thus, integrating practical training and realistic simulations into cybersecurity education represents an opportunity for participants to engage in practical cybersecurity practices [25, 104, 105, 106, 103].

5.3.4 Role-Specific Training Approaches

Participants also mentioned a need for a cybersecurity training towards roles and responsibilities. They noted that cybersecurity trainings' effectiveness depends on the role of the professional, suggesting that there is a need for modular course structures that allow participants to educate themselves with the needed cybersecurity skill for their role. This finding supported by the cybersecurity competency framework [33], where the emphasis

lies on the respective role. Adopting a role-specific approach on top of cyber hygiene would support organisations to better address the diverse cybersecurity knowledge requirements of different professional groups. This approach would also support technological advancements and organisational needs [107].

5.3.5 International Standards and Regulatory Compliance Training

One participant suggested that training focused on international cybersecurity standards and regulatory compliance would help professionals and organisations to understand their roles and responsibilities better [38, 108, 35, 109].

5.3.6 Supply Chain Security Training

Given the significant risks posed by supply chain vulnerabilities, training programs specifically addressing supply chain security management are essential. Participants emphasised the need for training that covers supplier vetting, risk assessment methodologies, and continuous monitoring of supply chain risks. Training should also include practical guidance on implementing secure supply chain practices, conducting supplier audits, and managing third-party cybersecurity risks effectively [110].

5.3.7 Risk Management Training

Participants mentioned varying approaches regarding cybersecurity risk management practices. Mainly, participants mentioned resource constraints as a barrier for planning risk management within their organisations [111, 49].

5.3.8 Collaboration Between Academia, Space Industry, and Cybersecurity Experts

The participants expressed their concern regarding to the lack of expertise in the field of space cybersecurity. This finding goes parallel with the industry professionals' perspective report [63]. By supporting collaboration across academia, space industry, and cybersecurity experts, organisations can ensure that cybersecurity education remains up to date. Collaborative approaches would also facilitate the development of training methodologies, practical exercises, and a specialised content tailored to space cybersecurity [112, 113, 114].

5.4 Validation

The questions were validated from the participants' responses by asking for feedback throughout the data collection process. Also, Triangulation method was used, which is a method used in validation, checking responses from multiple participants and questions to find patterns. This method improves the reliability of qualitative findings by comparing them [91].

Participants rated their cybersecurity knowledge between 2 and 8, with an average score of 5.25 (Figure 1). Only two participants reported receiving formal cybersecurity training in the past year (Figure 3). The distribution of scores showed no clear grouping, indicating varied knowledge levels (Figure 4). Participants described their perceived cybersecurity knowledge as ranging from basic awareness ("brief article," "basic phishing training") to specialised knowledge ("cryptography," "heavy monitoring," "ISO-related measures"). This validated the perceived cybersecurity knowledge as their answers supported their capabilities of discussing complex topics. As the self rating scores increased, the complexity of the responses respectively increased, showing positive correlation. Also, comparison of multiple data points (correlation coefficient, answer overlap, and response distribution) (Q2: "Have you received any formal cybersecurity training in the last 12 months?" Q6: "Is regular cybersecurity training mandatory for employees in your organisation?") It provides an evidence that organisational training policies directly influence individual training experiences in cybersecurity contexts. Also, comparison of another data points; A high correlation (0.77) was found between participants who had not received cybersecurity training and those whose organisations did not require cybersecurity training (Figures 6, 7). This finding does not necessarily mean that the participants are unaware, or there is a bad practice, but rather points a gap in existing specialised cybersecurity training and in regulations. Participants emphasised the need for specialised cybersecurity knowledge tailored to space systems. The quantitative data supports the qualitative statements about the need for specialised, industry-specific cybersecurity training, as all of the participants expressed their interest in specialised training.

External validation was obtained from 5 space cybersecurity experts. Experts validated the applicability and the necessity of the proposed training topics. Also, space cybersecurity experts emphasised the importance of practical applications the most, indicating most of the resources available regarding to the space cybersecurity focuses too much on theory. One expert mentioned the value of basic cybersecurity training for the smaller companies, since they tend to have resource limitations, but they are also important for the supply chain as they are part of it. One emphasised the necessity of supply chain management training, since level of sophistication is much higher in the space industry. Overall, feedback

obtained from all of experts were highly positive, indicating that the suggestions are applicable and valuable.

5.5 Limitations

The study was limited to space industry professionals working in Estonia. This directly limited the number of participants available. Small sample size, may limit the generalisability of the results. Second, sensitivity of the topic may have effected the responses. Additionally, time constraints posed a challenge. Each limitation is explained in detail.

The scope of the study was limited to assessing the perceived cybersecurity knowledge and cybersecurity knowledge gaps to provide suggestions for training areas. While this focus was necessary to maintain the feasibility of the study, within the timeline and resources, it restricted the findings and their applications. First, cybersecurity knowledge levels should have been assessed, as TNA methodologies suggests assessing the necessity of the training in the first step [72]. Especially, perceived cybersecurity knowledge levels should have been assessed, since assessing cybersecurity knowledge would have needed whole another approach and study design. The study relied on a small sample of professionals, which may not fully represent the entire industry. Also, it should be acknowledged that small number of participants affects statistical data significantly, potentially skewing overall scores and limiting the generalisability of the findings. Therefore, caution should be taken when interpreting and applying these results broadly across the space sector.

The research conducted in this thesis involved sensitive information regarding organisations' cybersecurity practices. This sensitivity may influence the willingness of participants to share insights and practices. Even though participants' identities were anonymised, by human nature it can be difficult to acknowledge mistakes, if any were made. Additionally, bad practices could have significant impacts on security, especially when discussing vulnerabilities or knowledge gaps. To mitigate this challenge, all interviews and surveys were conducted in accordance with strict confidentiality protocols. However, the possibility of partial disclosure or self-censorship may still apply.

Finding meaningful participants for the study, and setting dates for interviewing participants posed a challenge. Given the niche nature of the Estonian space industry and the limited number of organisations operating in this domain, finding eligible participants required significant effort. Scheduling interviews with busy executives posed a challenge. This limitation was tackled by prioritising their availability and comfort. After successfully finding space industry professionals in Estonia, finding space cybersecurity experts for validation presented another major challenge. Fortunately, this step had been anticipated

and was therefore carefully planned and resolved by participating in an international conference on space cybersecurity to validate the results.

5.6 Future Expectations and Estonia's Potential Role

Participants agreed upon cybersecurity would become increasingly critical in the space sector over the next five years, providing reasonable arguments. The growing number of satellites, increased reliance on space based services, and evolving geopolitical threats show the need of addressing cybersecurity vulnerabilities proactively.

Estonia, with its strong reputation in cybersecurity and IT innovation, is uniquely positioned for a leading role in space cybersecurity. Participants highlighted Estonia's potential to become a European centre for space cybersecurity expertise, leveraging existing strengths in cybersecurity education, research, and industry collaboration. Developing specialised training programmes, research initiatives, and industry standards could position Estonia as a global leader in securing space infrastructure.

6. Recommendations

This chapter provides recommendations for tailored cybersecurity training to the space industry in Estonia. Based on the analysis and discussion presented in this study, actionable recommendations are proposed. These recommendations address educational gaps by introducing training needs. These training needs proposed for building specialised expertise, and improve the levels of cybersecurity knowledge.

6.1 Improve Overall Cybersecurity Levels by Cyber Hygiene

Improving general cybersecurity levels by basic cyber hygiene in the space industry is essential to mitigate human related vulnerabilities. Regular awareness campaigns and introductory training courses should be implemented to form a foundational cybersecurity knowledge among all industry personnel regardless of their role. Providing introductory cybersecurity courses accessible to all employees, emphasising basic cyber hygiene is recommended. The course should include the topics of secure file management, password practices and phishing training, secure communication practices, data handling procedures, and recognising and responding to common cyber threats is recommended. Also, those trainings should be regularly updated to adapt evolving threats [103].

6.2 Develop Specialised Cybersecurity Education and Training Programmes

Current cybersecurity training programmes are generic and do not specifically address the operational characteristics and vulnerabilities of satellites and space infrastructure. Thus, the programme should integrate cybersecurity principles with space specific technical knowledge, addressing areas such as satellite vulnerabilities, space communication protocols, onboard computer security, and orbital mechanics [63, 53].

6.3 Implement Practical Cybersecurity Training

Participants emphasised the importance of practical, based on real world applications in a training. Regular training sessions utilising realistic simulations and cyber ranges can significantly improve cybersecurity knowledge levels. It is recommended to develop and regularly update these realistic scenarios tailored specifically to space systems. Also,

evaluating cybersecurity threats from an attackers perspective can provide valuable aspects for understanding attack methodologies [115, 25, 104, 105, 106].

6.4 Develop Supply Chain Security Training

Given the significant risks associated with supply chain vulnerabilities, it is recommended to develop training programmes specifically focused on supply chain management. Additionally, practical guidance should be provided on implementing secure supply chain practices and managing third-party cybersecurity risks proactively [110].

6.5 Develop Risk Management Training

The study identified the need for training in risk management specific to cybersecurity incidents affecting space systems. Participants noted that some organisations within the space sector may lack structured processes for effectively managing cyber incidents. Training programmes should therefore focus on developing clear incident response plans, roles and responsibilities for cyber incidents, communication protocols, and recovery procedures [111, 49].

6.6 Develop International Standards and Regulatory Compliance Training

The importance of training in accordance with international cybersecurity standards, regulatory compliance was identified. Training programmes regarding to the legal aspects of cybersecurity is recommended. Also, the training programme should include both compliance requirements, and the regulatory landscape [38, 108, 35, 109].

6.7 National and International Stakeholder Collaboration

Collaboration between universities, industry, and government agencies is recommended to design specialised curricula and introduce dedicated courses in space cybersecurity at higher education institutions. Forming a partnerships among academia, industry, and government would support knowledge exchange and training opportunities. Also, cybersecurity threats in the space sector requires international collaboration and information sharing. Supporting international collaboration for space cybersecurity is recommended. Additionally, encouraging industry, government, and academic participation for collaboration in global level for standardised international cybersecurity frameworks, regulations and protocols for strengthening cyber resilience is recommended [53, 112, 114, 113].

6.8 Leadership in Space Cybersecurity

Estonia's strengths in digital technologies and cybersecurity position has already set a foundation for leading role in space cybersecurity education. Promoting Estonia as a regional hub for space cybersecurity research and training is recommended. Promoting international collaboration will further enhance Estonia's leadership role [25].

7. Conclusion

This thesis was specifically designed to assess training needs for cybersecurity in the space industry in Estonia by conducting a TNA. While the participants' perceived cybersecurity knowledge varied, it is acknowledged that basic cybersecurity knowledge is needed regardless of the role. This finding shows that there is a growing awareness of cybersecurity risks among professionals in the space industry in Estonia. However, this awareness has not yet translated into practical applications, as most participants have not received formal cybersecurity training. Also, some companies' approaches to cybersecurity were rather reactive, with measures implemented only after incidents occur or when required by regulation. This practice gap may stem from the absence of regulations and policies mandating cybersecurity training and the lack of expertise between the domains of cybersecurity and space. The research reveals that most professionals and organisations acknowledge the existence of vulnerabilities but may lack the resources or technical understanding to address them effectively. Although the need for cybersecurity is widely recognised, there is a significant gap in specialised knowledge. Many professionals express a need for tailored training and education special to space and cybersecurity. As the current training opportunities and university curricula do not sufficiently address these needs, this may leave the industry vulnerable to both known and unknown threats. Thus, universities must develop specialised training within their curricula collaborating both nationally and internationally.

This thesis identified several topics that should be prioritised in future cybersecurity courses, including foundational cybersecurity knowledge, building on that, specialised cybersecurity content for space and role specific training approaches. Also, practical training and realistic applications were recommended. Addressing these priorities represents a significant opportunity to improve cybersecurity resilience within the space sector. However, addressing these challenges requires a proactive approach and collaboration between policymakers, government, industry and academia.

This includes developing specialised training programmes, integrating cybersecurity into space and systems engineering education, and supporting proactive risk management and a culture of continuous learning. Regarding to that, the following actionable steps are recommended:

1. Universities, in collaboration with industry experts, should develop and implement

foundational cybersecurity courses. These courses should be mandatory for all professionals entering the space sector, regardless of their specific roles, to ensure they understand cybersecurity principles and cyber hygiene practices.

2. Building upon foundational knowledge, universities should collaborate with industry stakeholders and cybersecurity experts to design specialised curricula integrating cybersecurity principles with space-specific technical knowledge.
3. Industry and academia should jointly develop practical, hands-on training programmes and realistic simulation exercises. Scenario-based training tailored to space systems will improve students' and professionals' practical cybersecurity skills.
4. The industry should conduct regular assessments of cybersecurity competencies and report to academia. These assessments will help identify evolving knowledge gaps and training needs, and by reporting to academia, training programmes will remain relevant and practical.
5. Policymakers and government agencies must develop clear regulations and policies mandating cybersecurity training and compliance within the space industry. Regulatory frameworks should encourage cybersecurity practices and continuous professional development, thus supporting a culture of cybersecurity awareness.
6. Estonian universities and research institutions should actively seek collaboration with leading space universities globally. Supporting knowledge exchange, joint curriculum development, and shared research initiatives, would improve the quality of cybersecurity training programmes. Collaborative efforts will also position Estonia as a central hub for space cybersecurity education and innovation.

Global cooperation is needed, and Estonia has an opportunity to possess essential expertise in space cybersecurity by investing in specialised training programmes, and developing collaborations. By doing so, Estonia can efficiently use its strengths in IT, setting an example for other countries and contributing to the resilience of the global space ecosystem.

8. Further Research

To effectively address cybersecurity challenges within the space sector, it is essential to identify specific training needs and conduct targeted research to inform tailored educational initiatives. Initially, a foundational cyber hygiene training course should be developed to establish baseline cybersecurity knowledge among professionals. Additionally, a specialized space cybersecurity program should be created, integrating core cybersecurity principles with space-specific technical expertise.

Beyond theoretical knowledge, practical cybersecurity training and simulation exercises are crucial to ensure professionals can effectively respond to real-world scenarios. Further research should explore effective methodologies for developing these specialized training programs, particularly scenario-based training, to enhance cybersecurity preparedness within the space sector. Such research will provide valuable insights and best practices to guide the design and implementation of future cybersecurity education initiatives.

Moreover, future studies should be conducted over extended periods and involve larger sample sizes to accurately assess cybersecurity competencies and training effectiveness. Regular assessments of cybersecurity knowledge are also necessary to continuously monitor professionals' knowledge gaps and evolving training needs. Implementing these regular evaluations will support ongoing professional development, strengthen cybersecurity capabilities, and promote a proactive security culture within the space sector.

References

[1] International Organization for Standardization. *ISO/IEC 27001:2022 Information Security Management Systems – Requirements*. Available at: https://www.iso.org/standard/82875.html. 2022.

[2] National Institute of Standards and Technology (NIST). *Framework for Improving Critical Infrastructure Cybersecurity*. Accessed: 2025-04-09. 2023. URL: https://www.nist.gov/cyberframework.

[3] National Initiative for Cybersecurity Careers and Studies (NICCS). *Explore Terms: A Glossary of Common Cybersecurity Words and Phrases*. Accessed: 2025-05-12. 2024. URL: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary#letter-c.

[4] European Union Agency for Cybersecurity (ENISA). *ENISA Threat Landscape Report 2023*. Accessed: 2025-04-09. 2023. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

[5] IBM Security. *IBM X-Force Threat Intelligence Index 2024*. Accessed: 2025-04-09. 2024. URL: https://www.ibm.com/security/data-breach/threat-intelligence.

[6] U.S. Department of Homeland Security. *Critical Infrastructure Security and Resilience*. Accessed: 2025-04-09. 2023. URL: https://www.dhs.gov/critical-infrastructure-security.

[7] IBM. *What is Critical Infrastructure?* Accessed: 2025-05-11. URL: https://www.ibm.com/think/topics/critical-infrastructure.

[8] RAND Corporation. *National Security Research Division Annual Report*. Accessed: 2025-04-09. 2023. URL: https://www.rand.org/nsrd.html.

[9] Academy to Innovate HR (AIHR). *A Guide to Conducting a Training Needs Analysis*. Accessed: 2025-04-08. 2022. URL: https://www.aihr.com/blog/training-needs-analysis/.

[10] Netherlands Aerospace Centre (NLR). *Training Needs Analysis (TNA)*. Accessed: 2025-04-08. 2024. URL: https://www.nlr.org/training-needs-analysis-tna/.

[11] Juan Racionero-Garcia and Siraj Ahmed Shaikh. "Space and cybersecurity: Challenges and opportunities emerging from national strategy narratives". In: *Space Policy* 70 (2024), p. 101648. DOI: 10.1016/j.spacepol.2024.101648.

[12] Center for Security Studies. *Space Security in an Insecure World*. https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSSAnalyse343-EN.pdf. 2023.

[13] Shafqat Hameed, Ahmad Raza, and Junaid Tariq. "Working and Applications of Global Positioning System". In: *Journal of American Science* 7.10 (2011), pp. 51–57. URL: https://www.jofamericanscience.org/journals/am-sci/am0710/007_6362am0710_51_57.pdf.

[14] USAF Shaun R. Stuger Lt Col. *SPACE BASED INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE CONTRIBUTION TO GLOBAL STRIKE IN 2035*. Tech. rep. AD1018137. Defense Technical Information Center. Air University, Air War College, 2012. URL: https://apps.dtic.mil/sti/pdfs/AD1018137.pdf.

[15] Gregory Falco. "Cybersecurity Principles for Space Systems". In: *Journal of Aerospace Computing, Information, and Communication* 16.2 (2018). Accessed: September 30, 2024, pp. 1–10. URL: https://www.researchgate.net/publication/329596980_Cybersecurity_Principles_for_Space_Systems/citations.

[16] Royal Australian Air Force. *Space Power Manual*. Accessed: September 30, 2024. 2022. URL: https://www.airforce.gov.au/sites/default/files/2022-09/213304_space_power_emanual_v1.0a%5B1%5D.pdf.

[17] Ulpia Elena BOTEZATU. *Cybersecurity in the Era of Space Domain Awareness*. https://rocys.ici.ro/documents/116/Art._3_ROCYS_1_2024.pdf. 2024.

[18] AFCEA International. "Evolving Cybersecurity Landscape: Space - The New Frontier for National Security". In: *SIGNAL Magazine* (2019). Accessed: 2024-10-08. URL: https://www.afcea.org/signal-media/cyber-edge/evolving-cybersecurity-landscape-space-new-frontier-national-security.

[19] Viasat Inc. *KA-SAT Network Cyber Attack Overview*. Mar. 2022. URL: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview.

[20] David E. Jackson. "ASAT Goes Cyber". In: *Proceedings* (Feb. 2021). Accessed: November 5, 2024. URL: https://www.usni.org/magazines/proceedings/2021/february/asat-goes-cyber.

[21] Trade with Estonia. *Estonia signs cooperation agreement with NASA*. Accessed: 2024-12-27. 2024. URL: https://tradewithestonia.com/estonia-signs-cooperation-agreement-with-nasa/.

[22] Madis Võõras. *Estonia's Bold Journey in Space: From Emerging to Established Space Nation*. https://tradewithestonia.com/estonias-bold-journey-in-space-from-emerging-to-established-space-nation/. Accessed: 2025-04-30. 2024.

[23] Enterprise Estonia (EAS). *SCS Range RFI Report*. Accessed: September 30, 2024. 2023. URL: https://eas.ee/wp-content/uploads/2023/03/scs-range-rfi.pdf.

[24] Research in Estonia. *The Security of Satellites Has Been Dangerously Neglected*. Accessed: September 30, 2024. Aug. 2024. URL: https://researchinestonia.eu/2024/08/29/satellites-security/.

[25] European Space Agency. *ESA support building Estonia's space cyber range*. Accessed: 2025-03-02. 2024. URL: https://connectivity.esa.int/news/esa-support-building-estonia%E2%80%99s-space-cyber-range.

[26] NASA. *NASA welcomes Estonia as newest Artemis Accords signatory*. Accessed: 2024-12-27. 2024. URL: https://www.nasa.gov/news-release/nasa-welcomes-estonia-as-newest-artemis-accords-signatory/.

[27] CMOE. *Training Needs Analysis – Definition*. Accessed: 2025-05-13. URL: https://cmoe.com/glossary/training-needs-analysis-definition/.

[28] Capitol Technology University. *Should Space be United States' 17th Critical Infrastructure?* Accessed: 2025-03-02. 2024. URL: https://www.captechu.edu/blog/should-space-be-united-states-17th-critical-infrastructure.

[29] European Defence Fund. *Indicative Multiannual Perspective 2025-2027*. Accessed: 2025-03-02. 2025. URL: %5BInsert%20URL%20if%20available%5D.

[30] Jacob G. Oakley. *Cybersecurity for Space: A Guide to Foundations and Challenges — Second Edition*. Apress; Second edition (17 July 2024), 2024.

[31] European Union Agency for Cybersecurity (ENISA). *Cybersecurity Skills Development in the EU*. Available at: https://www.enisa.europa.eu/publications/cybersecurity-skills-development-in-the-eu. 2020.

[32] European Union Agency for Cybersecurity (ENISA). *European Cybersecurity Skills Framework (ECSF) - User Manual*. Accessed: 2025-03-10. 2022. URL: https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20User%20Manual.pdf.

[33] National Cybersecurity Centre (CNCS). *Cybersecurity Competencies Framework*. Tech. rep. Accessed: 2025-03-10. National Cybersecurity Centre (CNCS), 2022. URL: https://www.cncs.gov.pt/docs/cybersecurity-competencies-framework-cncs.pdf.

[34] Jean Barbazette. *Training Needs Assessment: Methods, Tools, and Techniques*. Accessed: 2024-10-08. URL: %5Curl%7Bhttps://www.slideshare.net/slideshow/training-needs-assessment-methods-tools-and-techniques-jean-barbazette-zliborgpdf/252007410#22%7D.

[35] Madi Gates. *Houston, We Have a Problem: International Law's Inability to Regulate Space Exploration*. Accessed: 2025-05-08. 2025. URL: https://nyujilp.org/houston-we-have-a-problem-international-laws-inability-to-regulate-space-exploration.

[36] Joan Johnson-Freese. *Space Warfare in the 21st Century: Arming the Heavens*. 1st. Routledge, 2016.

[37] James Clay Moltz. "The Changing Dynamics of Twenty-First-Century Space Power". In: *Strategic Studies Quarterly* 13.1 (2019), pp. 50–75. URL: https://www.jstor.org/stable/26585375.

[38] Du Li. *Global Governance of Space Cyber Security: Regulatory and Institutional Aspects*. 1st. Routledge, 2025. DOI: 10.4324/9781003561996.

[39] Aisha Adeyeri and Hossein Abroshan. "Geopolitical Ramifications of Cybersecurity Threats: State Responses and International Cooperations in the Digital Warfare Era". In: *Information* 15.11 (2024). ISSN: 2078-2489. DOI: 10.3390/info15110682.

[40] NASA. *Orion Radiation Handout*. 2014. URL: https://www.nasa.gov/wp-content/uploads/2015/11/np-2014-03-001-jsc-orion_radiation_handout.pdf.

[41] Australian Bureau of Meteorology. *Guide to Space Radiation*. URL: https://www.sws.bom.gov.au/Category/Educational/Space%20Weather/Space%20Weather%20Effects/guide-to-space-radiation.pdf.

[42] Juan A. Fraire, Oana Iova, and Fabrice Valois. “Space-Terrestrial Integrated Internet of Things: Challenges and Opportunities”. In: *IEEE Communications Magazine* 60.12 (2022), pp. 64–70. DOI: 10.1109/MCOM.008.2200215.

[43] Jonathan Kua et al. “Internet of Things in Space: A Review of Opportunities and Challenges from Satellite-Aided Computing to Digitally-Enhanced Space Living”. In: *Sensors* 21.23 (2021), p. 8117. DOI: 10.3390/s21238117.

[44] Edward Smith. “Implementing Cybersecurity Solutions for Space Network Protection”. In: *CSIAC Journal* 9.1 (Feb. 2025). URL: https://csiac.dtic.mil/articles/implementing-cybersecurity-solutions-for-space-network-protection/.

[45] David Livingstone and Patricia Lewis. *Space, the Final Frontier for Cybersecurity?* Tech. rep. Accessed: 2025-03-10. Chatham House, The Royal Institute of International Affairs, 2016. URL: https://www.chathamhouse.org/2016/09/space-final-frontier-cybersecurity.

[46] James Pavur and Ivan Martinovic. “Building a launchpad for satellite cyber-security research: lessons from 60 years of spaceflight”. In: *Journal of Cybersecurity* 8.1 (June 2022). ISSN: 2057-2085. DOI: 10.1093/cybsec/tyac008.

[47] Mattias Wallén. *The Future of Space Cybersecurity: A New Era of Threats and Innovations*. Swedish Space Corporation. Mar. 2025. URL: https://sscspace.com/the-future-of-space-cybersecurity-a-new-era-of-threats-and-innovations/.

[48] Sarah Mahmood. *Critical Infrastructure Vulnerabilities to GPS Disruptions*. Presentation at the National Space-Based Positioning, Navigation, and Timing Advisory Board Meeting, Homeland Security Advanced Research Projects Agency Science & Technology Directorate. Accessed: 2025-04-30. June 2014. URL: https://www.gps.gov/governance/advisory/meetings/2014-06/mahmood.pdf.

[49] Brandon Bailey. *Establishing Space Cybersecurity Policy, Standards, and Risk Management Practices*. Tech. rep. The Aerospace Corporation, 2020. URL: https://aerospace.org/sites/default/files/2020-10/Bailey%20SPD5_20201010%20V2_formatted.pdf.

[50] Rhonda Farrell. *Cybersecurity-by-Design: Building Resilient Agencies*. Accessed: 2025-05-09. Jan. 2025. URL: https://www.govloop.com/community/blog/cybersecurity-by-design-building-resilient-agencies/.

[51] Shah Khalid Khan et al. “Space cybersecurity challenges, mitigation techniques, anticipated readiness, and future directions”. In: *International Journal of Critical Infrastructure Protection* 47 (2024), p. 100724. ISSN: 1874-5482. DOI: https://doi.org/10.1016/j.ijcip.2024.100724.

[52] Hillevi Nilsson Linnea Palmqvist. “A Multidisciplinary Analysis of Cyber Security in the Swedish Space Industry”. PhD thesis. Uppsala University, 2022. URL: https://uu.diva-portal.org/smash/get/diva2:1666846/FULLTEXT01.pdf.

[53] Jessica Dawson and Robert Thomson. “The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance”. In: *Frontiers in Psychology* 9 (2018). URL: https://api.semanticscholar.org/CorpusID:47021737.

[54] Johannes Willbold et al. “Space Odyssey: An Experimental Software Security Analysis of Satellites”. In: *Proceedings of the 2023 IEEE Symposium on Security and Privacy (SP)*. 2023, pp. 1–19. DOI: 10.1109/SP46215.2023.10351029.

[55] Finabel - European Army Interoperability Centre. *The Intersection Between Outer Space Security and Cybersecurity*. Accessed: 2025-03-10. 2023. URL: https://finabel.org/the-intersection-between-outer-space-security-and-cybersecurity/.

[56] Douglas Broom. *As private satellites increase in number, what are the risks of the commercialization of space?* 2022. URL: https://www.weforum.org/stories/2022/01/what-are-risks-commercial-exploitation-space/.

[57] Defense Intelligence Agency. *Challenges to Security in Space*. Accessed: 2025-03-10. 2022. URL: https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf.

[58] NASA Office of Inspector General. *Cybersecurity Readiness of NASA’s Ground Systems Supporting Space Launch System, Orion, and Exploration Ground Systems*. Tech. rep. IG-21-019. Accessed: 2025-04-30. NASA Office of Inspector General, June 2021. URL: https://oig.nasa.gov/wp-content/uploads/2024/02/ig-21-019.pdf.

[59] Cybersecurity and Infrastructure Security Agency (CISA). *Recommendations to Space System Operators for Improving Cybersecurity*. Tech. rep. Accessed: 2025-05-03. U.S. Department of Homeland Security, 2024. URL: https://www.cisa.gov/sites/default/files/2024-06/Recommendations%

20to%20Space%20System%20Operators%20for%20Improving%20Cybersecurity%20%28508%29.pdf.

[60] NATO Science and Technology Organization. *STO-MP-SAS-141-18:* Accessed: 2025-03-02. URL: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-OCS-ORA-2023/MP-SAS-OCS-ORA-2023-08.pdf.

[61] EU SST. *EU Space Surveillance and Tracking (EU SST)*. Accessed: 2025-05-03. 2025. URL: https://www.eusst.eu.

[62] NASA. *Space Traffic Management (STM) Architecture*. https://technology.nasa.gov/patent/TOP2-294. Accessed: 2025-05-03. 2025.

[63] The White House. *Space System Cybersecurity: Industry Perspectives Report*. Accessed: 2025-03-02. 2025. URL: https://bidenwhitehouse.archives.gov/wp-content/uploads/2025/01/Space-System-Cybersecurity-Industry-Perspectives-Report.pdf.

[64] Executive Office of the President. *Cybersecurity Principles for Space Systems*. https://www.federalregister.gov/documents/2020/09/10/2020-20150/cybersecurity-principles-for-space-systems. Accessed: 2025-05-03. Washington, D.C., 2020.

[65] European Union Agency for Cybersecurity (ENISA). *Cybersecurity for Space Infrastructure*. Available at: https://www.enisa.europa.eu/publications/cybersecurity-for-space-infrastructure. 2021.

[66] European Space Agency (ESA). *ESA Cybersecurity Policy and Guidelines*. Available at: https://www.esa.int/Safety_Security/Cybersecurity. 2020.

[67] European Space Agency. *SPACE-SHIELD: Space Attacks and Countermeasures Engineering Shield*. URL: https://spaceshield.esa.int.

[68] National Aeronautics and Space Administration. *Space Security: Best Practices Guide (BPG)*. 2024. URL: https://swehb.nasa.gov/display/SWEHBVD/7.22+-+Space+Security%3A+Best+Practices+Guide.

[69] Constructors Australia. *Training Needs Analysis*. Accessed: 2024-10-08. Constructors Australia, 2019. URL: https://www.constructors.com.au/wp-content/uploads/2019/11/Training-Needs-Analysis.pdf.

[70] Japan International Cooperation Agency (JICA). *Training Needs Analysis for the Capacity Development of the Core Human Resources in the Cambodian Water Supply Sector: Inception Report*. Japan International Cooperation Agency, 2006. URL: https://www.jica.go.jp/Resource/project/cambodia/0601331/pdf/english/3_TNA_01.pdf.

[71] U.S. Department of Education. *Comprehensive Needs Assessment*. Accessed: 2024-10-08. U.S. Department of Education, 2014. URL: https://www.ed.gov/sites/ed/files/admins/lead/account/compneedsassessment.pdf.

[72] World Meteorological Organization (WMO). *Training Needs Analysis: Guidelines for National Meteorological and Hydrological Services*. 2020. URL: https://etrp.wmo.int/mod/resource/view.php?id=8500.

[73] Society for Human Resource Management (SHRM). *How to Conduct a Training Needs Assessment*. URL: https://www.shrm.org/topics-tools/tools/how-to-guides/how-to-conduct-training-needs-assessment.

[74] V. A. S. H. Murthy. "Methods of Data Collection". In: *ResearchGate* (2018). URL: https://www.researchgate.net/publication/325846997_METHODS_OF_DATA_COLLECTION.

[75] G. P. H. van der Linden and P. F. M. D. M. van der Linden. *International Handbook of Survey Methodology*. Routledge, 2008. URL: https://www.researchgate.net/publication/46706288_International_Handbook_Of_Survey_Methodology_2008.

[76] ACAPS. *Questionnaire Design for Needs Assessment*. Accessed: 2024-10-08. ACAPS, 2016. URL: https://gbvaor.net/sites/default/files/2019-07/1607%20ACAPS%20Questionnaire%20Design%20for%20Needs%20Assessment.pdf.

[77] European Space Agency. *Estonia to host Europe's new space cybersecurity testing ground*. Accessed: 2025-03-02. 2024. URL: https://www.esa.int/Applications/Connectivity_and_Secure_Communications/Estonia_to_host_Europe_s_new_space_cybersecurity_testing_ground.

[78] e-Estonia. *Estonia: A European and global leader in the digitalisation of public services*. Accessed: 2025-03-02. 2023. URL: https://e-estonia.com/estonia-a-european-and-global-leader-in-the-digitalisation-of-public-services/.

[79] ERR Novaator. *Milline oli eestlaste panus Nõukogude Liidu kosmoseprogrammi*. Accessed: 2 March 2025. 2024. URL: https://novaator.err.ee/247566/milline-oli-eestlaste-panus-noukogude-liidu-kosmoseprogrammi.

[80] Krakul. *A Short History of the Estonian Space Industry*. Accessed: 2025-03-02. 2023. URL: https://krakul.eu/short-history-of-the-estonian-space-industry/.

[81] University of Tartu. *Estonia became a space country today – ESTCube-1 was placed into orbit*. Accessed: 2025-03-02. 2013. URL: https://ut.ee/en/content/estonia-became-space-country-today-estcube-1-was-placed-orbit.

[82] European Space Agency. *Member States welcome Estonia*. Accessed: 2025-03-02. 2015. URL: https://www.esa.int/About_Us/Corporate_news/Member_States_welcome_Estonia.

[83] NASA. *NASA welcomes Estonia as newest Artemis Accords signatory*. Accessed: 2025-03-02. 2023. URL: https://www.nasa.gov/news-release/nasa-welcomes-estonia-as-newest-artemis-accords-signatory/.

[84] Telecompaper. *Estonia to launch first commercial satellite in 2026*. Accessed: 2025-03-02. 2024. URL: https://www.telecompaper.com/news/estonia-to-launch-first-commercial-satellite-in-2026--1522539.

[85] European Space Agency. *ESA supports Estonia's first industry-led optical communication satellite*. Accessed: 2025-03-02. 2024. URL: https://connectivity.esa.int/news/esa-supports-estonia%E2%80%99s-first-industryled-optical-communication-satellite.

[86] Invest in Estonia. *Global Cybersecurity Index: Estonia is the #1 cybersecurity country in the EU*. Accessed: 2025-03-02. 2024. URL: https://investinestonia.com/global-cybersecurity-index-estonia-is-the-1-cybersecurity-country-in-the-eu/.

[87] Estonian Space Office. *Eesti kosmosepoliitika*. Accessed: 2025-03-02. 2015. URL: https://eis.ee/wp-content/uploads/2015/11/Eesti_kosmosepoliitika_A4_EST_web.pdf.

[88] Estonian Information System Authority (RIA). *Estonian Information Security Standard (E-ITS)*. https://www.ria.ee/en/cyber-security/management-state-information-security-measures/information-security-standard-e-its. Accessed: 2025-04-30. 2024.

[89] John W. Creswell and J. David Creswell. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. 5th ed. Accessed: 2024-11-30. Thousand Oaks, CA: SAGE Publications, 2018. ISBN: 978-1-5063-8670-6. URL: https://extranet.ogs.edu/ogsdial/upload/OXFORD/2024/2643/resources/Creswell_2018.pdf.

[90] Heba Maarouf. "Pragmatism as a Supportive Paradigm for the Mixed Research Approach: Conceptualizing the Ontological, Epistemological, and Axiological Stances of Pragmatism". In: *International Business Research* 12 (Aug. 2019), pp. 1–1. DOI: 10.5539/ibr.v12n9p1.

[91] Anthony J. Onwuegbuzie and R. Burke Johnson. "The Validity Issue in Mixed Research". In: *Research in the Schools* 13.1 (2006). Accessed: 2025-04-30, pp. 48–63. URL: https://citeseerx.ist.psu.edu/document?repid=rep1&type=pdf&doi=e3f3b024d30274821f4328b6bcd34ec96b7878c4.

[92] Steinar Kvale. *Doing Interviews*. The SAGE Qualitative Research Kit. Accessed: 2025-04-30. London: SAGE Publications, 2008. ISBN: 9780761949770. URL: https://www.karnacbooks.com/product/doing-interviews/32977/.

[93] Joe A. Castillo-Montoya. "The Interview Protocol Refinement (IPR) Framework: A Four-Phase Process for Improving the Quality of Interview Protocols in Qualitative Research". In: *The Qualitative Report* 21.5 (2016). Accessed: 2025-04-30, pp. 811–831. URL: https://nsuworks.nova.edu/cgi/viewcontent.cgi?article=2337&context=tqr.

[94] Edward Loper Bird Steven and Ewan Klein. *Natural Language Toolkit (NLTK)*. https://github.com/nltk/nltk. Accessed: 2025-04-30. 2025.

[95] Chintan Surfer. *rake-nltk: NLTK-based implementation of the Rapid Automatic Keyword Extraction algorithm*. https://github.com/csurfer/rake-nltk. Accessed: 2025-05-13. 2017.

[96] J. D. Hunter. "Matplotlib: A 2D graphics environment". In: *Computing in Science & Engineering* 9.3 (2007), pp. 90–95. DOI: 10.1109/MCSE.2007.55.

[97] Aric A. Hagberg, Daniel A. Schult, and Pieter J. Swart. "Exploring Network Structure, Dynamics, and Function using NetworkX". In: *Proceedings of the 7th Python in Science Conference (SciPy 2008)*. Ed. by Gaël Varoquaux, Travis Vaught, and Jarrod Millman. Pasadena, CA USA, 2008, pp. 11–15. URL: https://conference.scipy.org/proceedings/scipy2008/paper_2/.

[98] Wes McKinney. "Data Structures for Statistical Computing in Python". In: *Proceedings of the 9th Python in Science Conference*. Ed. by Stéfan van der Walt and Jarrod Millman. 2010, pp. 56–61. DOI: 10.25080/Majora-92bf1922-00a.

[99] pandas development team. *pandas.DataFrame.corr — pandas 2.2.3 documentation*. Accessed: 2025-04-30. pandas. 2024. URL: https://pandas.pydata.org/docs/reference/api/pandas.DataFrame.corr.html.

[100] Michael L. Waskom. "seaborn: statistical data visualization". In: *Journal of Open Source Software* 6.60 (2021), p. 3021. DOI: 10.21105/joss.03021.

[101] GDPR-info.eu. *Consent – GDPR*. https://gdpr-info.eu/issues/consent/. Accessed: 2025-05-06.

[102] Virginia Braun and Victoria Clarke. *Thematic Analysis: A Practical Guide*. Accessed: 2025-04-30. London: SAGE Publications Ltd, 2021. ISBN: 9781473953246. URL: https://uk.sagepub.com/en-gb/eur/thematic-analysis/book248481.

[103] Centre National D'études Spatiales. *Orbital System Cybersecurity Hygiene Guide*. Accessed: 2025-05-13. 2025.

[104] Nexova. *CITEF – The Cyber-Range Solution*. https://www.nexovagroup.eu/sites/default/files/media/files/2024-10/citef_brochure_oct_2024_digital_lr.pdf. Accessed: 2025-04-30. 2024.

[105] European Space Agency. *New cyber-security centre will safeguard ESA assets and missions*. https://www.esa.int/Space_Safety/New_cyber-security_centre_will_safeguard_ESA_assets_and_missions2. Accessed: 2025-04-30. 2021.

[106] European Space Agency. *ESA ESEC*. https://www.esa.int/About_Us/Corporate_news/ESA_ESEC. Accessed: 2025-04-30.

[107] Julie Haney et al. *Federal Cybersecurity Role-based Training Approaches, Successes, and Challenges*. US Department of Commerce, National Institute of Standards and Technology, 2023.

[108] Daniella Febbraro. "The Need for Cyber Resilience of Space Assets: Law and Policy, Considerations of Ensuring Cybersecurity in Outer Space". In: *21:1 CJLT 99*. 23 (2014). Accessed: 2025-04-30, pp. 91–104. URL: https://digitalcommons.schulichlaw.dal.ca/cgi/viewcontent.cgi?article=1308&context=cjlt.

[109] Ministry of Economic Affairs and Communications of Estonia. *Estonia gets a space law*. https://mkm.ee/en/news/estonia-gets-space-law. Accessed: 2025-04-30. 2024.

[110] Tomas Paulik. “Security Challenges of Complex Space Applications: An Empirical Study”. In: *arXiv preprint arXiv:2408.08061* (2024). Presented at the ESA Security for Space Systems (3S) conference, May 28, 2024. URL: https://arxiv.org/abs/2408.08061.

[111] Joint Task Force. *Security and Privacy Controls for Information Systems and Organizations*. NIST Special Publication 800-53 Revision 5. National Institute of Standards and Technology, 2020. DOI: 10.6028/NIST.SP.800-53r5.

[112] Indiana University. *The Nation's First Academic Space Cybersecurity Program Welcomes the 2nd Cohort*. https://www.cybersecuritydive.com/spons/the-nations-first-academic-space-cybersecurity-program-welcomes-the-2nd-co/711137/. Accessed: 2025-04-30. Mar. 2024.

[113] U.S. Space Command. *Academic Engagement Enterprise (AEE)*. Accessed: 2025-05-18. 2024. URL: https://www.spacecom.mil/Partnerships-and-Outreach/Academic-Engagement-Enterprise/.

[114] Seth Robbins. “Embry-Riddle Partners With Space ISAC to Elevate Space Cybersecurity Research and Education”. In: *Embry-Riddle Aeronautical University News* (2025). Accessed: 2025-05-18. URL: https://news.erau.edu/headlines/embry-riddle-partners-with-space-isac-to-elevate-space-cybersecurity-research-and-education.

[115] Romanian Ministry of National Defence. *Locked Shields 2024 Cybernetic Defence Exercise*. https://english.mapn.ro/cpresa/6225_Locked-Shields-2024-Cybernetic-Defence-Exercise. Accessed: 2025-04-30. 2024.

Appendix 1 – Non-Exclusive License for Reproduction and Publication of a Graduation Thesis[1]

I Elif Mihrişah Can

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Training Needs Analysis for Cybersecurity to the Estonian Space Industry", supervised by Dr. Adrian Venables and co-supervised by Anna Mandrenko.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

18.05.2025

[1]The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

Appendix 2 – Interview Transcript & Consent Form

Introduction

The purpose of this interview is to conduct a training needs analysis for cybersecurity training within the Estonian space sector. These questions will provide insight into cybersecurity knowledge and practises within the Estonian space industry. The interview is semi-structured to allow flexibility and follow-up based on the responses.

Interviewees

The list of interviewees is disclosed in this file.

General Instructions

The responses will remain confidential, and no personally identifiable information will be shared. The responses will be recorded only for analysing the answers and will not be shared anywhere or with any third party.

Background Information

a. Can you briefly describe your role and responsibilities within your organisation?
b. How long have you been involved in the Estonian space industry?

Interview Questions

1) Cybersecurity Knowledge

a) How would you rate your current knowledge of cybersecurity in the space industry on a scale from 1 to 10? (Q1)
b) Have you received any formal cybersecurity training in the last 12 months? (Q2)
c) What type of cybersecurity training, if any, have you received? (Q14)
d) Do you believe your current knowledge of cybersecurity is adequate for your role? (Yes/No) (Q3)

2) Cybersecurity Challenges

a) What are some of the main cybersecurity challenges you think the industry faces? (Q15)
b) Are there specific cybersecurity areas you feel need improvement within your organisation? (Q16)
c) Does your organisation have a dedicated cybersecurity team? (Yes/No) (Q4)
d) Is cybersecurity considered a priority in your organisation? (Yes/No) (Q5)
e) Is regular cybersecurity training mandatory for employees in your organisation? (Yes/No) (Q6)

3) Cybersecurity Risks

a) Does your organisation perform regular security audits? (Yes/No) (Q7)
b) Do you feel that your organisation is adequately protected against cyber threats? (Yes/No) (Q8)

4) Current Practises

a) What cybersecurity measures are currently in place in your organisation? (Q17)
b) How often does your organisation review or update these policies? (Q18)

5) Scenario Discussion: Cybersecurity Incident Involving Spacecraft

a) In your opinion, what would be the most likely method of exploiting a spacecraft's cybersecurity vulnerabilities? (e.g., hacking communication systems, exploiting software vulnerabilities, etc.) (Q19)
b) Could you describe a possible incident scenario? Q20)
c) If you were involved in responding to a cybersecurity incident with a spacecraft, what would be the first action you would take? (e.g., isolate the spacecraft, alert authorities, assess damage, etc.) (Q21)
d) Would you involve other organisations, such as space agencies or cybersecurity experts, in the response to the incident? (Yes/No) (Q9)

6) Training Needs

a) In what areas do you think additional training or resources are needed for cybersecurity in your industry? (Q22)
b) Would you be interested in attending a specialised course on cybersecurity for the space industry? (Q10)

7) Future Expectations

a) Do you think that cybersecurity will become more critical for the space industry in the next 5 years? (Yes/No) (Q11)
b) How do you see the role of cybersecurity evolving in the Estonian space industry over the next few years? (Q23)
c) Are there any specific topics or issues you believe should be prioritised in future cybersecurity courses? (Q24)
d) Would you support the development of a specialised cybersecurity training course for space industry professionals? (Yes/No) (Q12)

Feedback

- Could you share your general thoughts on the interview? Were there any areas that could be improved?
- Did you find the questions clear and easy to understand? (Yes/No)
- If no, which questions did you find unclear, and how can they be improved?
- Are there any additional questions you believe should be included to ensure a comprehensive understanding of the cybersecurity knowledge gaps?

Closing

Thank you for participating in this interview. Your insights are invaluable in helping us assess the current state of cybersecurity knowledge and identify areas for improvement.

Interview Consent Form

Master's Thesis Research

Researcher: Elif Mihrisah Can
Institution: Tallinn University of Technology
Department: Department of Software Science
Contact Information: elif.can@taltech.ee

Title of the Study: Training Needs Analysis for Cybersecurity to the Estonian Space Industry

Purpose of the Study:

The purpose of this interview is to conduct a training needs analysis for cybersecurity training within the Estonian space sector. These questions will provide insight into cybersecurity knowledge, practises and training needs within the Estonian space industry.

Procedures:

Participation involves an interview lasting approximately 30-60 minutes. The interview will be audio-recorded and transcribed for analysis. You may decline to answer any question or stop the interview at any time without any negative consequences.

Confidentiality:

All information collected during this interview will remain confidential. Your identity will be anonymised in any reports, publications, or presentations resulting from this research. Audio recordings and transcripts will be securely stored and accessible only to the researcher.

Voluntary Participation:

Your participation in this study is entirely voluntary. You have the right to withdraw at any point during or after the interview without providing a reason.

Contact Information:

If you have any questions or concerns about this study, please contact me directly at the email address provided above. If you have concerns about your rights as a participant, please contact Institutional Review Board or Ethics Committee.

Consent Statement:

I have read and understood the information provided above. I voluntarily agree to participate in this interview and consent to the audio recording of the interview. I acknowledge all or part of the content of the interview may be used in publications.

Participant's Name: _____

Participant's Signature: _____

Annex 1 – Interview Response Transcript

Interview Response Transcript

P1

Q: What are some of the main cybersecurity challenges you think the industry faces?

A: "Well, I can't get around Russia at the moment due to the war in Ukraine. The efforts that are being undertaken are so much less subtle and so much more direct. Basically every part of the system is vulnerable in some way. I think they're using all of the methods. So anything from tapping undersea cables to having students go through bachelors masters and doctorate programmes that end up in the industries, people, education, good job tech and then leverage using their family or parents at home to provide information on these companies and agencies. I definitely think that is inside vector. Satellites - You can't even upgrade or retract, so we're going to have a bunch of satellites up there, but they are going to become vulnerable in the next 10 years that we cannot upgrade. Some of the techniques that had been used on smaller scales, but they are pretty troubling. Various jamming techniques so that will be there was a multi month period, where we can land planes using GPS in Finland and I think near here as well, because the Russians were jamming the cheapest frequencies that can cause massive massive outages in various sectors. Basically anything with automatic navigation that we used. It all depends on the GPS, now all the new cars they are all dependent. So you can just buy denial of service for hours or days or even even weeks you can crash subsections of the economy. We have old satellites up there that have no security and they're mostly out of fuel. What you can also do is, even if you don't cause any damage, if you don't destroy it, you can de orbit it. I don't know that's kind of hopeless, hopeless issue. I look at it from the perspective, I'm looking at it from an attackers perspective."

Q: What cybersecurity measures are currently in place in your organisation?

A: "There are silos, regular reviews and updates, and heavy monitoring. Even if someone enters their password incorrectly, it will be investigated."

Q: How often does Your organisation review or update these policies?"

A: "It's the kind of thing that we do continuously. We do not have a specific process. Whenever we feel like a change is needed."

P2

Q: What are some of the main cybersecurity challenges you think the industry faces?

A: "In software engineering, the approach is more generic; they tend to use methods that work for hardware, so once something works, it is not changed. I believe they also apply this concept to software. Sometimes, I think, they deliberately avoid solving certain issues, even if they are aware of them, because any change would require re-certification. We had to fight a lot for our system in the past as well."

Q: How often does your organisation review or update these policies?"

A: "We do not have former policies."

Q: What cybersecurity measures are currently in place in your organisation?

A: "We use internal VPNs, with all traffic tunnelled. We do not expose internal devices to the outside, and we employ encryption. We also maintain a physical server, which is kept encrypted, as well as regular back-ups."

P3

Q: How often does Your organisation review or update these policies?

A: "Yearly."

P4

Q: What type of cybersecurity training, if any, have you received?

A: "[...] was the author of that, so it is more like they ask these first five questions, it is these kinds of questions that you definitely don't know the answers to. They prove that you don't know anything about cybersecurity. This is what we're doing almost every year. It is very basic training that covers phishing and that."

Q: What are some of the main cybersecurity challenges you think the industry faces?

A: "Definitely, there is a heavy underestimation. At first people were laughing at it like "this is not an issue why are you putting your energy on this?" And then, in 2022 the world was proved that everyone was shown through the Viasat satellite hack before the invasion of Ukraine. That this is an issue, and the space sector has heavy vulnerabilities in space that our space objects are not cyber secure and this is a very underestimated security issue that we have. Main challenge so far that the spacecrafts on orbit today, most of them are not cybersecure."

Q: In what areas do you think additional training or resources are needed for cybersecurity in your industry?

A: "Definitely, the space particularities and interdependencies. Heavily understudied area, especially in Europe. We don't have enough cybersecurity experts in the field of space. No cybersecurity experts teaching space communication systems. So teaching cyber security experts the particularities of space and space communication systems and studying how to detect hackings is very important."

P5

Q: What type of cybersecurity training, if any, have you received?

A: "A small course that is online, based on answering a questionnaire."

Q: What are some of the main cybersecurity challenges you think the industry faces?

A: "I would definitely name the legacy systems that many organizations rely on. Since many satellites have been deployed a long time ago, and the security protocols and information that have been added to those satellites are based on previous knowledge, not the current knowledge. Then, legacy systems pose major threats. And also, challenges are in the increasing level of attacks that can be made from different actors. And the general geopolitical environment since the situation in Europe and in different places in the world currently is quite unstable, then we are not sure what kind of actors and what kind of attacks will be put against the systems that we have."

Q: In what areas do you think additional training or resources are needed for cybersecurity in your industry?

A: "We can see that there is a need for space related projects and developments, especially within cybersecurity, then the knowledge that is required to be able to develop technical needs and trainings for cyber range is lacking. I would say that resources are limited and people available are also limited. And educating new developers to be knowledgeable in this field is beneficial, as well as for myself. And I believe learning about space and specific technological questions that are related to that is needed. I am planning myself to find courses or educate myself in any possible way on both space cybersecurity and as well the technical aspects of satellites and ground systems."

Q: Are there any specific topics or issues you believe should be prioritised in future cybersecurity courses?

A: "Currently, the cybersecurity courses are more generic, which is understandable since the industry works this way. But for satellites, the knowledge has to be pretty specific since the vulnerabilities that are applied to satellites are different from the generic ones. More specialised. It can be specific protocols that can be vulnerable to attacks or just the general knowledge of what kind of systems are the weakest in the satellites and what kind of advantages can be in protecting those systems as well as, what I'm saying, the technical aspects of both ground and satellite communications since these are, not the most generic knowledge, but a very specific one"

P6 Q: What type of cybersecurity training, if any, have you received?

A: "Thinking back, and maybe just some brief article that each university employee has to read - do not do this, try to not do that, and that's pretty much it. When I was in the [...] I remember getting some, I don't know, some cybersecurity people were doing some audits, and we just had a small article. I think it was a small article about how to set up two-factor authentication."

Q: Are there any specific topics or issues you believe should be prioritised in future cybersecurity courses?

A: "I think it all starts with basic cyber hygiene. Try to not reuse passwords and secure ground link or ground stations. I don't really think there is anything super specific that we need to do regarding satellites."

P7

Q: What cybersecurity measures are currently in place in your organisation?

A: "I think there isn't really a risk mitigation like a campaign in that kind of in the [...] So, current practices as I already mentioned about the two-factor authentication seem to be one of the best ways to get a large amount of people to have more security against password leaks. Then at least the two-factor authentication helps it a bit, so that seems to work."

Q: How often does your organisation review or update these policies?

A: "I do not know about policies. This is a new thing about like reviews and policies of cyber securities. I have no idea currently. We do not really have reviews in the [...], and we don't have really a policy. Yeah, there should be a policy for you to read or update them."

Q: In what areas do you think additional training or resources are needed for cybersecurity in your industry?

A: "The regular training should be mandatory because whatever I did in bachelors I have already forgotten regarding most of the infrastructure access for example how to do SSH properly and all these things we kind of do it with some simple way but well I think it's important to have once in a year or at least once a year every two years some kind of a training that would keep everyone on the same page, like what you should do, what you shouldn't do, how to do it properly and all that."

Q: Are there any specific topics or issues you believe should be prioritised in future cybersecurity courses?

A: "What was lacking that people didn't know what is space, how does space work and I think that was quite a thing that is needed, that sort of education is needed and even space people, space engineers, not always know the orbital mechanics."

P8

Q: What cybersecurity measures are currently in place in your organisation?

A: "We do security testing. We match our security credentials, or let's say they are strictly controlled. We also apply industry-based practices where possible while developing our services. We do not have written policies for every potential situation. Not enough resources for us."

Q: In what areas do you think additional training or resources are needed for cybersecurity in your industry?

A: "I think the overall level of cybersecurity must be raised, as in other industries as well. So, educate people to understand what is happening and how to protect themselves and the industry as such. Then, of course, certain people need more exposure to the specifics as well."

Q: Are there any specific topics or issues you believe should be prioritised in future cybersecurity courses?

A: "It depends on the audience. If you take a wider audience from the space sector, it's basics. Or basically, it has huge impact, I think."

P9

Q: What are some of the main cybersecurity challenges you think the industry faces?

A: "All those software defined radios, many old space systems against more actors. US, Europe against Russia China, they really seem to be wanting to do bad things. Actually trying to harm cables underseas, satellites also, with bad actors, definitely."

Q: Are there any specific topics or issues you believe should be prioritised in future cybersecurity courses?

A: "it would have to be very practical and pragmatic. If you say we need more defence, that doesn't do anything for me, hypothetical scenarios of hacking a satellite doesn't do anything for me, because, i think i have a better understanding how hard it is in practice. so you have to engage me, it would have to be realistic in other words.Just theoretical slides of hypothetical scenarios, it's very easy to dismiss in my psychology."

P10

Q: What are some of the main cybersecurity challenges you think the industry faces?

A: "The space sector is one of the last industrial domain where cybersecurity is being introduced. Therefore, the key risk is that the industrial ecosystem is not fully ready in

managing overall security incidents, from the identification up to the response and recovery measures. This include not only their corporate activities, but also the security of the space assets once in operations. One further point that is critical is the management of the supply chain, which may pose serious risks to space assets and missions."

Q: In what areas do you think additional training or resources are needed for cybersecurity in your industry?

A: "More in general, it is missing a job figure that mixes expertise on both cyber and space system engineering."

P11

Q: Are there any specific topics or issues you believe should be prioritized in future cybersecurity courses?

A: "I suspect that the technologies and techniques involved are not widely known or understood outside specialist circles. Across the entire space industry, I do not think this knowledge is widespread. It seems to me that it remains highly specialised, with only certain individuals within companies or organisations possessing the necessary expertise and dealing with these matters. It is not really a general knowledge."

P12

Q: In what areas do you think additional training or resources are needed for cybersecurity in your industry?

A: "I think there's probably multiple layers of training that they would find useful. One just awareness of the different ways, that a cyber attack could look like and different types of cyber attack."

Q: Are there any specific topics or issues you believe should be prioritized in future cybersecurity courses?

A: "As I mentioned with an overview, something on protecting, actual data and images. Something on protecting the data centres and data access. Really everything. An introduction course."