CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Security Studies

Master's Thesis

2023 **Michaela Dvořáková**

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Security Studies

Tackling Cybersecurity Threats to the EU Space Programme: Regional and International Cooperation

Master's thesis

Author: Michaela Dvořáková

Study programme: Bezpečnostní studia – Bezpečnost, technologie a společnost

Supervisor: Mgr. et Mgr. Jakub Pražák

Year of the defence: 2023

Declaration

1. I hereby declare that I have compiled this thesis using the listed literature and resources only.
2. I hereby declare that my thesis has not been used to gain any other academic title.
3. I fully agree to my work being used for study and scientific purposes.

In Prague on
03.05.2023

Michaela Dvořáková

References

DVOŘÁKOVÁ, Michaela. *Tackling Cybersecurity Threats to the EU Space Programme: Regional and International Cooperation.* Prague, 2023. 106 pages. Master's thesis (Mgr.). Charles University, Faculty of Social Sciences, Institute of Political Studies. Department of Security Studies. Supervisor Mgr. et Mgr. Jakub Pražák.

Length of the thesis: 116 804 characters

Abstract

Cyber-attacks to various sectors have been on the rise over the past decade, and the EU space programme is not exempt to these. Due to many European industries and sectors relying heavily on space-enabled systems, maintaining the security and availability of EU space is key for the proper function and prosperity of the EU and its competitiveness. With the emergence of New Space, space-based systems are becoming more connected to the internet, creating more vulnerabilities which can be exploited by cyber-attackers. However, space-based objects are not the only segment of the EU space programme that are vulnerable to exploitation. Space cybersecurity has not been on the forefront of researcher's focus, until now. The past decade has shown a shift in attention towards the issue of space cybersecurity, but this mainly focuses outside of the EU. This research aims to find out how cyber threats to the EU space programme have evolved throughout the past decade and how they have been tackled within the EU. Regional and international cooperation on the matters of space cybersecurity of the EU space programme will be explored through the optic of identity building through shared threat. Research interviews with experts from the field of EU space programme cybersecurity shed light on the current situation, geopolitical significance, and possibilities for cooperation for a more secure EU space programme. Finally, this thesis will discuss key findings of the thematic analysis of research interviews and studied literature, which may help in the future development of cooperation in securing the EU space programme from cyber threats.

Abstrakt

Kybernetické útoky na různá odvětví v posledním desetiletí narůstají, a kosmický program EU není v tomto trendu výjimkou. Vzhledem k tomu, že mnoho evropských sektorů a průmyslových odvětví se silně spoléhá na kosmické systémy, je zachování bezpečnosti a dostupnosti kosmického programu EU klíčem k řádnému fungování a prosperitě EU a její konkurenceschopnosti. Se vznikem ‚New Space' se kosmické systémy stále více propojují s internetem, což vytváří více zranitelností, které mohou zneužít kybernetičtí útočníci. Kosmické (orbitální) objekty však nejsou jediným segmentem kosmického programu EU, který je zranitelný vůči zneužití. Kybernetická bezpečnost kosmického sektoru nebyla až dosud v popředí zájmu výzkumníků. Poslední desetiletí však naznačuje posun pozornosti výzkumníků směrem k otázce kybernetické bezpečnosti ve kosmu, ale prozatím se výzkum zaměřuje především mimo EU. Tato diplomová práce si klade za cíl zjistit, jak se kybernetické hrozby působící na kosmický program EU vyvíjely během uplynulého desetiletí a jak byly v rámci EU řešeny. Regionální a mezinárodní spolupráce v otázkách kybernetické bezpečnosti kosmického programu EU bude prozkoumána optikou budování identity prostřednictvím sdílené hrozby. Výzkumné rozhovory s odborníky z oblasti kybernetické bezpečnosti kosmického programu EU osvětlují současnou situaci, geopolitický kontext a možnosti spolupráce pro bezpečnější kosmický program EU. V závěru se tato práce bude zabývat klíčovými poznatky ze studia literatury a tematické analýzy výzkumných rozhovorů, které mohou pomoci v budoucím rozvoji spolupráce při zabezpečení kosmického programu EU před kybernetickými hrozbami.

Keywords

Space Cybersecurity, Cyber Threat, Space Security, Cybersecurity, EU space programme, EU Regional Cooperation, International Cooperation.

Klíčová slova

Vesmírná kybernetická bezpečnost, kybernetická hrozba, vesmírná bezpečnost, kybernetická bezpečnost, kosmický program EU, regionální spolupráce EU, mezinárodní spolupráce.

Název práce

Řešení kybernetických hrozeb pro vesmírný program EU: regionální a mezinárodní spolupráce

Acknowledgement

First and foremost, I would like to express my sincere gratitude to my thesis supervisor, Mgr. et Mgr. Jakub Pražák, for his guidance and encouragement throughout this project.
I am extremely grateful to my significant other, friends, and family, who provided me with undying support. Thank you for always being there for me when I needed it the most!
Finally, I would like to express my gratitude to each and every interview participant I had the honour to work with.

List of Abbreviations

CCDCOE	NATO Cooperative Cyber Defence Centre of Excellence
CERT	Computer Emergency Response Team
CPA	Competent PRS Authority
CGI	Consultants to Governments and Industry
DDoS	Distributed Denial of Service
DoS	Denial of Service
EC	European Commission
EEAS	European External Action Service
EGNOS	European Geostationary Navigation Overlay Service
ENISA	EU Agency for Cybersecurity
EP	European Parliament
ESA	European Space Agency
ESPI	European Space Policy Institute
EU	European Union
EUMETSAT	European Organisation for the Exploration of Meteorological satellites
EUSPA	EU Agency for the Space Programme
GPS	Global Positioning System
GSA	European GNSS Supervisory Authority
IRIS²	Infrastructure for Resilience, Interconnectivity and Secure by Satellite system
IT	Information Technology
ITU	International Telecommunication Union
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organisation
NIS 2	Network and Information Systems
NSA	National State Authority

PRS	**Public Regulated Service**
R&D	**Research and Development**
SATCOM	**Satellite Communications**
Space ISAC	**Space Information Sharing and Analysis Centre**
STM	**Space Traffic Management**
TRL	**Technology Readiness Level**
UN	**United Nations**
UNOOSA	**United Nations Office for Outer Space Affairs**

Table of Contents

1. INTRODUCTION

In a world that is incessantly more interconnected through the internet, it is important to start analysing all of its components to determine any possible less-than-optimally secure areas. Many newly produced and developed technologies already fulfil cybersecurity standards set by relevant institutions. Though, until not long ago, cybersecurity threats to space programmes were not recognised as a fatal issue, with the elevated levels of interconnectivity, academics and policymakers are increasingly focusing their efforts on securing one of the most important sectors - space.

Cybersecurity threats are constantly on the rise and their effect on the space sector is becoming progressively more noticeable. Not only are they on a rise, but the attacks are becoming more sophisticated. The complex geopolitical situation also gives way to competition for a dominant position within the international system, and cyber warfare is an efficient way to attack adversaries, due to its wide range of effects and well-known issue with attribution. The aim of this research is to find out how cyber threats to the European Union (EU) space programme have evolved throughout the past decade and how they have been tackled within the EU. Furthermore, the question regarding the cultivation of regional and international cooperation on the matters of space cybersecurity of the EU space programme will be discussed. It is necessary to focus academic research onto the topic of space cybersecurity, due to the rapid advance in technological development, but not enough academic research on the topic to mitigate the emerging threat.

This Master's thesis is divided into two sections: the theoretical and the analytical section. Within the theoretical section, the author of this thesis first introduces the research design, where the combined use of existing literature analysis as well as research interviews comes together to subsidise the existing research gap on space cybersecurity, especially within the EU space programme. Furthermore, the ethical aspects of the research are thoroughly explored, along with the limitations to the conducted research and possibilities of further research on the topic of space cybersecurity in the EU. Moreover, the author introduces the theoretical framework of Collective Identity and European Identity building based on common threats - in the case of this research - cyber threats and introduces existing literature on the studied topic.

The analytical part explores the geopolitical context of the issue of space cybersecurity and key topics uncovered during the research interviews with five participants from various institutional backgrounds. All complete interview transcripts are available as a part of this thesis. The interviews are supplemented with the study of existing literature, EU regulations and strategies, as well as publicly available audio-recordings of online events and conferences on the topic of space cybersecurity. The analytical part is divided into 7 thematic areas identified during the thematic analysis of the conducted research interviews and a results discussion section. These thematic areas are obtained directly on responses given by research interview participants, giving a well-rounded perspective on the current state of space cybersecurity of the EU space programme.

2. LITERATURE REVIEW

2.1 Defining terms

This thesis works with the terms space security and cybersecurity on a frequent basis, which is why it is necessary to define these to ensure that the terms are being comprehended in the way that the researcher intended. Space security, in the case of this thesis, encases all segments relevant to the EU space programme, and does not solely focus on orbital systems. This includes the ground systems segment, communications segment, user segment, as well as the space-based / orbital systems segment. (European Commission, 2023) Cybersecurity therefore affects not only the orbital technologies, but also all the other components, which comprise standard IT equipment comparable to any other company. (Manulis et al., 2020)

The EU space programme should also be clearly defined. According to the European Commission, the EU space programme *"implements space activities in the fields of Earth Observation, Satellite Navigation, Connectivity, Space Research and Innovation."* (European Commission, 2022) This is done through a tight cooperation between the European Space Agency (ESA), European Commission (EC), EU Agency for the Space Programme (EUSPA), European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT), EU member states, and various other key actors, both public and private. The current flagship programmes of the EU space programme (European Commission, 2022) are the following:

- Galileo - European Global Navigation and Positioning system
- Copernicus - European Earth Observation system
- EGNOS - European Geostationary Navigation Overlay Service system

- Govsatcom - European Governmental Satellite Communication Service system
- STM - European Space Traffic Management system
- IRIS^2 - Infrastructure for Resilience, Interconnectivity and Secure by Satellite system

These flagship programmes are of great importance to the EU; however, some need different, higher levels of security than others. Communication constellations, for example, need a higher level of security than Earth observation constellations, due to the security implications that even a short denial of service could have. Therefore, some of the aforementioned EU space programmes will need a heightened protection from cyber-attacks.

In terms of cybersecurity, this thesis works with the simple definition that it comprises any attempts to create safe and secure information systems - this includes keeping secure from cyber threats all the hardware, software, and employees of, in the case of this thesis, the EU space programme. The attacks may be *"purely criminal. Others are espionage, often but not always state-sponsored. Yet others are potentially disruptive or destructive, again often but not always state-sponsored."* (Libicki, 2016:129) However, the definition used throughout this thesis includes not only external malicious interference, but also possible user or insider mistakes or malicious cyber acts.

Moreover, the concepts of regional and international cooperation in the case of this thesis need to be defined in order to set the boundaries between the two, while also setting the scope to regional cooperation. By regional, this thesis understands the cooperation between member states of the EU, also including the United Kingdom due to its involvement in the EU Space Programme. By international, this thesis means global cooperation, also including the EU member states and the United Kingdom.

2.2 Existing Cyber Threats and Vulnerabilities to the EU Space Programme

Depending on the source, there are different divisions to the segments within space programmes which need to be secured. Some sources state that the ground segment, the communications segment, the user segment, and the orbital / space segment are all significant and in need of being secured from unintended or malicious cyber interference. (European Commission, 2023; King & Goguichvili, 2020) However, there may be other views on the division; a source states up to 5 segments, including the launch segment in addition to the aforementioned. (New Space Economy, 2023) The researcher made the decision to conform to the division by the European Commission for the purpose of this research, thus meaning the division into the Ground segment, communications segment, user segment and the orbital segment.

2.2.1 Distinguishing Cyber x Electronic Warfare

This thesis works with the term cyber threats in attachment to some aspects of electronic warfare. Though the two are commonly distinguished as two separate types of attack, *"electronic warfare (EW) and cyber warfare are becoming conflated as the electro-magnetic environment merges with cyberspace."* (Ball & Waters, 2013:95) Cyber warfare and electronic warfare are complementary; through the combination of both, there have been observations of effective and dynamic long-term offensive strategies, which can make adversaries all the more dangerous. (Tadjdeh, 2018; Porche et al. 2013) For example, it is possible to *"transmit computer code to inject it into an adversary's network,"* (Theohary & Hoehn, 2019:1) which shows the clear convergence of both disciplines. Furthermore, many of the research interview participants do not distinguish between electronic and cyber-attacks, but rather use the term cyber threats as an umbrella term for both electronic and cyber-attacks acting on the security of the EU space programme infrastructure. What could elsewhere be categorised as an electronic attack, for example jamming and spoofing, is in this thesis categorised under the aforementioned umbrella term of ‘cyber-attack’.

2.2.2 Ground Systems Segment

Many components of the ground segment of the EU space programme are very similar to that of any other larger company or institution. For example, the technologies in the control stations; this means that they are sensitive to the same, or similar cyber threats as other sectors. These threats include DDoS (distributed denial of service) attacks, ransomware, phishing attacks, social engineering, as well as outdated or unpatched software, physical attacks, and more. (European Parliament, 2022; Manulis et al. 2020) According to publicly available sources, the systems which are used are heavily secured to prevent any unwanted interference, and the employees must undergo security clearances at respective National State Authorities (NSA) as stated by official hiring procedures of the EUSPA, as well as any other EU institution, when handling confidential information. (European Commission, 2006) Furthermore, the software used in command stations can be vulnerable to cyber-attacks, as it rarely has high military-grade security if not used for military purposes. (Peeters, 2022)

Some of the components, however, are quite different from those used in the control centres or monitoring centres. The ground stations, radio dishes or parabolic reflectors, are classified under the ‘ground segment’. (Cerqueira et al., 2013) However, due to the specifics of the communication between the Earth and space-based technologies, the risks and vulnerabilities of the communication segment will be discussed separately below.

2.2.3 Communications Segment

Though sometimes also classified within the ground segment, there are some specifics to this technology that diverge it from the purely ground systems. The communication segment comprises large antennae - radio dishes or parabolic reflectors - commonly called which enable communication between the ground-based systems and the space-based systems. (NASA, 2022) The communications segment is responsible for *"transmitting information (such as command and control instructions for orbital corrections) and receiving information (such as telemetry data about where the satellite is located),"* (Toukebri, 2021) in other words, enabling and maintaining the uplink, crosslink, and downlink. Satellite communication can be attacked, and the communications jammed, to make the satellite itself unavailable, or used to broadcast incongruous material. (Steinberger, 2008:26)

Attacks on the communications segment can be done namely through jamming or spoofing. Jamming could be described as an attack where *"transmitting a high-power electronic signal causes the bit error in a satellite's uplink or downlink signals to increase, resulting in the satellite or ground station losing lock."* (Zielinski et al, 1996:25) Spoofing, which could be understood as a 'sturdier' version of jamming, could be defined as an interference, where the attackers aim to take control of the satellite's transmission by camouflaging themselves as authorised users. This has been observed for example with the GPS. (Black, 2008:5) The above-mentioned interferences are usually not intended to harm the satellite, though the interference and loss of connection to the satellite can lead to a loss of information, money, or data. If the loss of connection between the ground and the satellites would become more lasting, in the case of a crisis it could lead to a loss of valuable information, which then could lead to a ‘tipping of scales’. Another harmful attack, aimed at gaining valuable information, is called ‘eavesdropping’ - essentially, the communication line is intercepted, and the attacker has access to all communications through the attacked channel. (Manulis et al., 2020)

2.2.4 User segment

The user segment then *“receives and uses the acquired data, e.g., scientists, media, agricultural companies and government.”* (Cerqueira et al., 2013:37) It includes predominantly widely used technology. The user segment and user terminals are often one of the most vulnerable openings to the cybersecurity of any system, as they are used by people with generally little to no advanced cybersecurity education or training. (MacGibbon, 2009) The lack of cybersecurity training is a common issue in many sectors, but as the space sector is vital to the functioning of other sectors, this makes it increasingly important to educate and train people in proper cybersecurity practices. The vulnerabilities here include both the users and the potentially faulty or vulnerable IT equipment, which could create a space through which an attacker could pass. For example, Manulis et al. (2020) explain that *“unpatched/outdated/legacy COTS software deployed among the platform is a known attack surface.”* (2020:7)

2.2.5 Space-Based Systems - Orbital Segment

While malicious actors can choose from a multitude of ways to attack a satellite in orbit, cyber-attacks pose a quite specific threat. They can not only temporarily disable, steal information from, or take control of satellites, but they can do so more stealthily, competently, and efficiently than other forms of attack.

While it is possible to permanently disable a satellite using a cyber-attack, it is not commonly practised, as it is not usually the primary objective of the attacker. (Black, 2008) A malicious actor can perform a variety of cyber-attacks, usually to take over the satellite (hijack it), or temporarily disable its functions, and similarly to other cyber-attacks, this is done predominantly for financial gain. According to research done by Santamarta in 2018, there were large numbers of aircraft, military bases and maritime vessels which could be accessed using unprotected or vulnerable SATCOM services. He analysed and described the types of vulnerabilities, which included *"backdoors, insecure protocols, and network misconfigurations."* (Santamarta, 2018:1) The satellites in orbit may be attacked by *"sending malformed data packets, [which] could lead to buffer overflows and create denial-of-service conditions to jam communications."* (Manulis et al., 2020:8)

2.2.6 Known Exploitations of Space Cybersecurity Weaknesses

In 2022, a space cybersecurity weakness was exploited in the midst of the War in Ukraine. Though some information on the ViaSat KA-SAT attack was made public, not all details are publicly available. However, from the information, which is freely accessible, modems with possible unpatched vulnerabilities were shut down and inoperable, and many people lost their satellite coverage. Most substantially, the Ukrainian army, government, and security services lost their communications throughout the beginning of the Russian invasion. (CCDCOE, 2022) Furthermore, the effects of the cyber-attack were visible all over Europe, and *"as of May 2022, thousands of customers were still left without internet* *connection."* (Poirier, 2022:6) The KA-SAT cyber-attack was one of the most large-scale attacks to be recorded in Europe recently. (CCDCOE, 2022) Moreover, Elon Musk's SpaceX, providing its Starlink terminals as aid to Ukraine, also had to face a considerable number of cyber-attacks, arguably led by Russia to put Ukraine at a disadvantage. (Howell, 2022)

One of the most publicly discussed exploitation of space cybersecurity weaknesses was performed by the cyber attackers commonly called 'Turla'. (Housen-Couriel, 2015:116) The notorious Russian hacker group has been named after the software they use, under the name of 'Epic Turla'. (Khandelwal, 2015) The Turla group used a variety of methods to hijack a satellite to mask their malicious activities. The group only attacked connections that were satellite-based, orbital, and only chose satellites that were covering the area of Africa and the Middle East. (Tanase, 2015) The satellite hijacking operation was performed by Turla mainly for the unique opportunity to gain *"sensitive data from government, military, diplomatic, research and educational organisations in the United States and Europe*" and additionally to *"hide their command-and-control servers from law enforcement agencies."* (Khandelwal, 2015) The aforementioned cyber-attacks were, however, eventually uncovered and gained high media coverage throughout the year 2015. Research shows that the Turla group has been active since 2007, which raises several additional questions about the timeframe during which sensitive information could have been stolen and leaked. (Tanase, 2015)

Moreover, there are other internationally recognised issues, such as the vulnerability of the Global Positioning System (GPS) against spoofing or jamming. (Westbrook, 2019; Goward, 2017) GPS is a widely used navigational system and can be found in a large variety of technologies, *"used to aid navigation in vehicles, it supports critical infrastructure by* *synchronising a wide range of computer-based systems, including for law enforcement, emergency services, transportation, communications, electrical power grids, and financial transactions, amongst many others."* (Westbrook, 2019:1) Due to this, it is vital to uphold a high level of protection of satellite navigation systems, so that they can provide both reliable and efficient performance. When attackers carry out a spoofing attack, *"false data [is] injected into a target's communications systems, fooling the receiver - GPS - into calculating an incorrect position."* (King & Goguichvili, 2020) Significant issues can arise if satellite navigation systems, especially when used by critical infrastructure, become unreliable and untrustworthy. There are many vulnerabilities of the GPS which have been repeatedly exploited, which is why there should be strong strategies on how to avoid these issues implemented within flagship EU space programmes, such as Galileo.

Studying real life examples of employing jamming as a form of cyber-attack on an adversary, *"it can be assumed that Russia, North Korea, and China jam neighbouring countries knowing that lethal retaliation is extremely unlikely, making jamming a low-risk, high-reward option if provocation is the intention."* (Westbrook, 2019:8) Jamming as a type of cyber-attack by foreign actors is a relatively common way to, for example, lower morale during military operations. This shows that it should be a priority to fix these vulnerabilities and attempt to secure the systems well enough to avoid the frequency of these attacks in the future. An example of this cyber-attack happened in 2014, was a *"momentary GPS interference [which] was considered a likely cause of two large ships colliding in Germany's busy Kiel Firth waterway."* (Westbrook, 2019:8)

What remains thought-provoking is that, though it became relatively somewhat widespread knowledge that the GPS can be spoofed, action has yet to be taken at an adequate level. Being recognised as an international security issue, discussed prevalently in the U.S.

media, especially with connection to Russia, which stated in 2016 that *"it had equipped over 250,000 cell towers with GPS jamming devices."* (Goward, 2017:18) This points to the shortcomings of the protection of the GPS against electronic warfare, which could be an issue of the EU programme Galileo, too, in the future.

2.3 The EU Regulatory Framework and the Governance of Cybersecurity in Space

In recent years, there have been increasing efforts to understand and protect assets from cyber threats. Despite these efforts, it could be claimed that the advance has not been fast enough, especially when considering the accelerating growth of cybercrime in the past decade. To many policymakers and academics, it became recognised that *"neither space policy nor cybersecurity policy is prepared for the challenges created by the meshing of space and cyberspace."* (Fidler, 2018:2) This claim has been supported through research conducted by Bailey et al, who state that *"overarching governance and policies lack the necessary integration between cybersecurity and the space domain."* (Bailey et al., 2019:4)

However, it is still important to reiterate that *"neither public nor private space asset organisations are at a complete standstill concerning their cybersecurity efforts,"* where the change in perception of cyber threats, especially to space-based assets, could be noticed. (Shadbolt, 2021:7) Below, the perception of cyber threats to the EU space programme will be illustrated through the close study of the EU legal and regulatory framework on the governance of cybersecurity threats to the EU space programme.

To understand more clearly the current state of space cybersecurity of the EU space programme, it is necessary to have knowledge of the current EU regulatory framework on the governance of EU space cybersecurity. Under the establishing document of the EUSPA, EU Regulation 2021/696 establishing the Union Space Programme and the European Union Agency for the Space Programme, which replaced and further developed the GSA (European GNSS Supervisory Authority), the official EU space programme was created. Additionally, it divides responsibilities and governance among three key actors: the European Commission, EUSPA, and ESA. In the case of the EU space programme, the EC is the main institution governing it, the EUSPA acts as an operational manager of various flagship programmes, along with ensuring the security accreditation for the EU space programme, and the ESA is mainly responsible for the R&D[1] component to the EU space programme. (Publications Office of the EU, 2022)

According to Article 34 of the EU Regulation 2021/696 establishing the Union Space Programme and the European Union Agency for the Space Programme, "*the Commission shall, in its field of competence and with the support of the Agency, ensure a high degree of security with regard, in particular, to:*

(a) the protection of infrastructure, both ground and space, and the provision of services, particularly against physical or cyber-attacks, including interference with data streams."

(EU Regulation 2021/696:109-110)

However, it is each Member state's own responsibility to ensure the integrity of their own ground systems and security of their infrastructures in relation to the EU space programme. (EU Regulation 2021/696:110) In terms of the regulation of cybersecurity, the establishing document further states that *"the cybersecurity of European space infrastructures, both ground and space, is key to ensuring the continuity of the operations of*

[1] Research and development

the systems and service continuity. The need to protect the systems and their services against cyber-attacks, including by making use of new technologies, should therefore be duly taken into account when establishing security requirements." (EU Regulation 2021/696:78) This point clearly states the rising importance of cybersecurity within the EU space programme, and that there are steps being taken in order to mitigate the emerging threat.

It is important to state that the issue of cybersecurity has been discussed in the EU in the past, especially in terms of the EU relationship to the ESA and its implications to overall EU space security. Nonetheless, there are only a few official EU documents that would focus on space cybersecurity prior to the establishing document of the EU space programme and the EUSPA.

Elaborating on the current state of cybersecurity regulation within the EU space programme, in 2022, the recently released Strategic Compass for Security and Defence stated security objectives for the EU, where space was determined as a strategic domain. It further stated a need for the development of a 'EU Space strategy for security and defence' in order to *"enhance [EU] ability to anticipate threats, guarantee secure access to strategic domains and protect [EU] citizens."* (EEAS, 2022:12) The EU Space Strategy was released in March of 2023, calling for changes in EU space law, the creation of an EU Space Information Sharing and Analysis Centre (ISAC), better cooperation and partnerships, and development of new technologies in order to transform EU space into a more secure and effective programme. (European Commission, 2023)

The EU space programme benefits from international cooperation. However, an issue arises from cooperation between Member States of the EU and ESA, as a part of the EU space programme. A 2012 communication from EC to the EP and the Council of the EU states that *“relations between EU and ESA are constrained by the fact that ESA's membership includes States not members of the EU, which poses an obvious problem in general and an even more acute problem when it comes to security and defence matters.”* (COM/2012/0671) Currently, the EU increasingly collaborates on issues regarding cybersecurity alone, for example CERT-to-CERT (Computer Emergency Response Team) information sharing arrangements internationally (Hitchens & Goren, 2017), or the CERT-EU for EU cybersecurity matters. This encloses all major cybersecurity incidents in the EU, also including cybersecurity incidents within the space sector. (CERT-EU, 2023)

Furthermore, there is international cooperation under the International Telecommunications Union (ITU), an agency of the United Nations, on securing the communication frequencies and satellites from unwanted or hostile interference. (Falco, 2018) Moreover, the United Nations Office for Outer Space Affairs (UNOOSA), figures as a platform of international cooperation, albeit hurdles to effective policy-making processes. (Baseley-Walker in Baylon, 2014) The cooperation, both within the EU and globally, aids the EU space programme in having a faster response time to cyber threats. (European Commission, 2023; ESPI, 2018) In the analytical part, the cooperation between ESA non-EU members and EU members is discussed, as well as the benefits of international cooperation weighed against its possible disadvantages.

2.4 A New Centre of Focus

Many authors have stressed the need for spreading awareness on the importance of space cybersecurity. One of the first authors focusing on space cybersecurity, Zielinski (1996), hypothesises about threats to space assets in the year 2025 where he correctly assumed that cyber threats would be an issue to space programmes. Academic research on this topic was scarce until about a decade ago, as has been explained earlier, which makes this piece of academic research quite unique in terms of its awareness and foresight on issues that the EU space programme is facing. Currently, more research and academic literature is appearing on the topic. It has become clear that space is an indispensable domain, which connects many aspects of everyday life, and thus needs even greater security. For example, Fidler (2018) discusses how cybersecurity is an emerging issue in need of resolution within space programmes in order to maintain an adequate level of security of space assets. Zatti (2017) analyses the way that space missions and assets have to be secured from hostile cyber behaviour. Additionally, Zatti mentions the appearance of new cybersecurity issues within EU space due to the emergence of New Space. (2017:8) Importantly, these sources help understand how an adequate level of cybersecurity can be acquired.

Furthermore, the works of Shadbolt (2021) and Santamarta (2018) help explain the technical side to the issue of space cybersecurity, in order to understand how cyber-attacks can target and influence space assets. Authors from the think-tank Chatham House, such as Livingstone & Lewis (2016), map the existing cyber threats and vulnerabilities which may influence space programmes. Baylon (2014) explains different countries' individual space programmes' and institutions' perspectives on the issue of space cybersecurity, which are important in order to understand the overall level of cooperation between countries on the topic. Poirier (2022) then explains the effects that an insecure space environment may have on European society. Weeden and Samson (2020) compiled a report on different countries' counter-space capabilities and found out that *"a growing number of non-state actors are actively probing commercial satellite systems and discovering cyber vulnerabilities that are similar in nature to those found in non-space systems."* (Weeden & Samson, 2020:17) The emergence of many academic articles, monographs, and policy recommendations on the topic of space cybersecurity show greater overall interest in the topic, though prevalently focused on space-based assets.

The importance of security of space-based assets from cyber-attacks was demonstrated multiple times in the past years, with one of the more prominent push-factors for change in focus towards space cybersecurity in the EU being the ViaSat KA-SAT attack amidst the War in Ukraine. (Poirier, 2022) Soon after, the Strategic Compass called for a comprehensive space security strategy. (EEAS, 2022) The EU Space Strategy for Security and Defence show-cased the shift in focus of the EU on the security of space, including space cybersecurity issues. (European Commission, 2023) Most recently, in April 2023, a cybersecurity test was performed by a Thales ethical hacking team on a ESA space-based asset, OPS-SAT, specifically for the third annual CYSAT conference. The results, which were used for illustrative purposes, showed that it was possible to exploit various vulnerabilities and gain access to control of the nanosatellite. (Thales, 2023) This shows an evident shift toward a more cybersecurity-focused, practical, and responsible approach to secure the EU space programme from cyber threats.

3. THEORETICAL FRAMEWORK

The research for this thesis will be conducted and analysed using the optic of identity building through shared threat. Cybersecurity as an international issue became more pronounced as technologies advanced. Space has recently been proclaimed as a strategic domain in the EU (EEAS, 2022), and as the fifth operational domain for NATO (NATO, 2022). Identity building through shared threat could explain, to a certain extent, the development of collective actions taken to mitigate the effects of cyber threats to the EU space programme.

3.1 Collective Identity and the Integration Theory

Firstly, it is necessary to develop a proper definition of collective identity, and how it will be used throughout this thesis. Collective identity is, according to social constructivism, formed through long-term processes. Wendt (1994) discusses that cooperation between states does not come naturally, it is constructed by long-term incidental or casual interaction (prevalently neutral-to-positive) between states. (1994:385) The collective identity can be formed through various different processes, and this subchapter will discuss the socio-psychological and sociological emergence of this concept, as well as its appearance in the realm of international relations and security studies. Furthermore, European integration and European identity will be discussed as an auxiliary factor to the formation of a collective identity.

From a sociological point of view on collective identity, Eisenstadt and Geisen (1995) introduce a model for analysis of the concept of collective identity, comprising of the following points:

1. *“Collective identity is not naturally generated but socially constructed: it is the intentional or non-intentional consequence of interactions which in turn are socially patterned and structured.” (1995:74)*
2. *“Collective identity is produced by the social construction of boundaries.” (1995:74)*
3. *“Constructing boundaries and demarcating realms presuppose symbolic codes of distinction, which enable us to recognise differences in the fluidity and chaos of the world.” (1995:74)*
4. *“The construction of boundaries and solidarity is not, however, a purely 'symbolic' affair, unrelated to the divisions of labour, to the control over resources and to social differentiation.” (1995:76)*
5. *“Primordiality is the first ideal type of collective identity.” (1995:77)*
6. *“The second major code of construction of collective identity is the ‘civic’ one.” (1995:80)*
7. *“A third type of code links to the constitutive boundary between ‘us and them’ not to natural conditions, but to a particular relation of the collective.” (1995:82)*

This model of analysis explains, fundamentally, the topic of collective identity and how it forms regardless of physical, naturally occurring, or other existing boundaries. Collective identity of the European Union, as in integrative process, can be explained using this theoretical model of analysis and following all its steps; from collective identity being simply a social construct due to artificially created boundaries to the 3 ideal types of collective identity.

Another, more socio-psychological perspective on the formation of collective identity can be observed through the theory on the formation of in-groups and out-groups through the Social Identity Theory, as introduced by Tajfel and Turner (1979). As Eisenstadt and Geisen (1995) also state in their work, there are boundaries that have to be constructed between 'us' and 'them'. Virtually, this means that there must be a process of division into groups in order to form a collective identity within the groups. (1995:82) However, this behaviour can be observed already in much smaller groups, and then projected onto larger groups, whole nations, or regional/international organisations. Essentially, the process of formation of these groups can be used to understand certain conflicts, including ones lead in cyberspace.

Cuhadar and Dayton (2011) try to demonstrate the existence of Social Identity Theory in practice, through analysis of different conflicts. They explain that *"human beings are, by nature, a pattern recognition species and that the human ability to distinguish between objects, circumstances, and behaviour is a functional cognitive process necessary for survival."* (2011:274) In-groups can, however, have their own divisions amongst themselves, especially if they become large enough, as proposed by Matonytė & Morkevičius (2009), *"collective views about potential threats might work in both directions: they might integrate and disintegrate a group."* (2009:969)

Correspondingly, the European Union, and Europe as a whole, can be classified as an in-group, in the terms that this thesis works with. Within this in-group, there may be other, smaller groups, but all belonging under this one umbrella of the EU. European integration has undergone many processes to get to the point it is currently at. Many scholars argue that, although Europe is interconnected, vastly due to institutionalisation and commercial ties, there is a loosely perceived collective European identity at the individual level, there rather exists one of allegiance to each person's respective nation-state. (Checkel and Katzenstein, 2009; Citrin and Sides, 2007) However, the gradual integration of European countries has slowly seeped into the minds of each European countries' nationals, where, in times of calm and prosperity, most Europeans believe that the European Union and its institutions are helpful in maintaining this state. On top of this, many Europeans identify themselves as both European nationals, and nationals of their respective countries; the two identities coexisting. (Fligstein et al., 2012; Hooghe and Marks, 2004)

The emergence of the European identity is also described in the works of Risse (2010), where the main consequences of the decades-long process results in the deepening and the widening of European identities. Risse emphasises that it is impossible to *"deduce a European identity from the fact that citizens from EU member states also hold EU citizenship"* (2010:20) and argues that *"some constructions of European identity have remained remarkably stable over the decades and even precede the European Union.*" (2010:21) Furthermore, throughout Risse's text it is implied that there are many identities within one person alone, leading to intertwining and/or conflicting identities, and projects itself from an individual to a group setting. (Risse, 2010) This discussion supports previous authors discussing the emergence of collective identity within the European Union.

This research assumes that the gradual build-up of institutional and commercial ties aids in building a collective identity. The co-dependency of European states in most matters, including those concerning the space sector, inevitably leads to the building of the collective

European identity. There are aspects to the European identity that most nationals seldom recognise on a regular basis, but aid in creating a whole. European integration has been (and still is) an uneven process, on many different levels. (Fligstein et al., 2012) The small, but significant advancements in cooperation between European states in different areas help build stronger connections. For example, the cooperation on new and emerging technologies, climate change, and other current topics may in return foster greater overall cooperation through more frequent communication.

However, institutional and commercial ties are not the only linkage to building a collective identity. Oftentimes, a collective identity is built also on other aspects of an individual's life; according to almost all determinants of one's own self. (Krasny, 2020:149) This had been displayed for example during the Covid-19 pandemic throughout the world, where unsafe surroundings led to overall enhanced cooperation to mitigate the threat of Covid-19. (Ścigaj, 2020:4) Experiences, over time, can change one's identity to fit closer to another, especially in times of great change or perceived threat. (Krasny, 2020:152) Consequently, due to overall unsafe circumstances, since cybersecurity issues can affect almost every sector, a collective identity could be built to face the common threat.

3.2 Identity Building Through Shared Threat

Construction of collective identity through a common threat could possibly explain the actions taken by states in order to mitigate cyber threats in a cooperative manner, just as it can explain the cooperation on many other issues. Though there will always be supporters and opposers of certain security measures put in place, there is, and will be, a gradual move toward a safer cyberspace. If the EU space programme is threatened by cyber-attacks, it will affect not only member states, but could possibly become a worldwide issue. The ripple effect that cybersecurity breaches can have on the EU space programme, or any other space programme in the world, could be devastating for various different sectors.

3.2.1 A Common Enemy

The common enemy plays a crucial role in the development of a collective identity. Once an enemy, be this a literal or a figurative one, poses a threat on an individual or a group, this can create or tighten existing bonds between a forming group. Many authors argue that *"group perceived threats are constitutive of collective identities."* (Matonytė & Morkevičius, 2009:969; Wendt, 1994; Risse-Kappen, 1995) This common enemy, posing different levels of threat, can be illustrated using a few of these following well-known examples.

Firstly, some global issues can unify society as a whole, such as terrorism and global warming. Though these two examples are fundamentally different, especially regarding the influence they have on the individual, they can both be viewed as hostile elements to the well-being of society. Terrorism is viewed often as an acute threat to an individual or a group's welfare with a lingering effect, whereas global warming tends to have a more mellow effect though having the potential to affect the entire population within a set timeframe. Additionally, the case of Covid-19 as the 'enemy' could be used to clarify the meaning of the common enemy, as used in this thesis. Again, this is not a specific individual or group posing the threat, it is rather a non-corporal 'enemy' which triggered a global response and managed to polarise the world into groups of supporters and opposers of implemented government health safety measures. (Ścigaj, 2020:2)

The role of the common enemy concept being explained, the use of this particular perception of it throughout this thesis will be regarding cyber attackers aiming to disrupt the proper performance of the EU space programme. Cyber attackers should be viewed as an out-group posing threat to the EU through attacking the EU space programme and limiting its full performance and potential and causing harm not only to the EU space programme itself, but to all which uses or benefits from the EU space technologies.

3.2.2 A Collective Response

Collective identity usually grows around the *"fear that the out-group has the capability or intention to inflict a negative consequence on the in-group."* (Rousseau & Garcia-Retamero, 2007) In reaction to a threat posed by the aforementioned 'common enemy', a collective response arises. Just as there are many levels of threats, there are many levels of response. The responses can vary greatly from more localised to global, and can be for example at a political, regulatory, or military level. These responses to the threat coming from the common enemy can create an environment under which a collective identity can form and become convalescent over time.

As will be discussed further throughout the analytical section of this thesis, the threat coming from cyber attackers to vital structures within the EU, such as the EU space programme, may lead to a creation of a collective identity in direct response. The collective response to this threat lies in the process under which governments and regulatory bodies *"universalize risk by making various threats mutual, and therefore the sense of danger, loss of trust, fear of what is unknown and new, become universal."* (Ścigaj, 2020:6)

4. RESEARCH DESIGN

The aim of the following chapter is to introduce the methodology of the research conducted for the purpose of this thesis. The research questions, justification of the selection of qualitative methods along with the limitations and ethical aspects of the conducted research will be discussed. Both primary and secondary sources were used to fulfil the needs of the research in order to answer the proposed research questions.

4.1 Research Questions

Space cybersecurity has come to be a part of scholarly research only about a decade ago. Although the focus within space security has been largely focused on other issues, policymakers started realising that this too is becoming a problem and could become even more-so in the future. There is still much research that needs to be conducted in the area of space cybersecurity. This thesis aims to find out how cyber threats to the EU space programme have evolved, how they have been tackled within the EU, and whether cyber threats to the EU space programme help EU member states cultivate regional and/or international cooperation in order to mitigate said threats through the following research questions:

RQ1: How have cyber threats to the EU space programme evolved in the past years? How have these threats been addressed within the EU?

RQ2: Do threats to the EU space programme from the cyber domain help member states foster regional and international cooperation in order to mitigate said threats?

The first research question aims to explore the development of space cybersecurity threats over the past decade, as most research on this topic appeared more prominently in approximately 2014, with disruptive Chatham House reports (Baylon, 2014; Livingstone & Lewis, 2016), bringing a closer focus on this specific emerging issue. This gives enough of a time frame to see whether there have been any clear trends in space cybersecurity threats. Furthermore, the second part of the first research question's objective is to explore the EU reaction to the observed trends, which could be extrapolated into the near future.

The second research question then aims to analyse whether space cybersecurity threats could foster cooperation. This will be explored through studying official material dispersed by EUSPA, as well as through interviews with chosen space cybersecurity professionals from both private and public institutions. Understanding the means of cooperation in the area of space cybersecurity is important for insight into the processes and discovering other possible means of cooperation in space cybersecurity.

4.2 Selection of Qualitative Methods and Methodology

The following subchapter follows the process of selection of qualitative methods and research interviews as a means to conduct research for the topic of this thesis. Furthermore, the methodology of research will be explained, along with the ethical component of researching with human participants. Lastly, the limitations to this research will be discussed.

4.2.1 Research Interviews

As had been mentioned before, there has not been enough research done yet in the field of space cybersecurity, though there has been an increase in public interest in the topic lately. (Livingstone & Lewis, 2016:8) The cybersecurity field quickly responds to threats, where patches or security software updates can quickly become threatened once again by inventive attackers. (Fouad, 2021) This results in rapid technological changes, to which policymakers seldom manage to react in time before more threats and changes appear. (ENISA, 2022) The research done on this topic is still extremely relevant, however, there are changes that the space cybersecurity field underwent which academics have not yet had the opportunity to react to or research. For this reason, the researcher chose to supplement the available literature with interviews from professionals from the field of space cybersecurity.

Research interviews have a long history in social science to be one of the cornerstones of qualitative research, where delving deep into the studied area along with a chosen participant often leads to obtaining valuable knowledge, often unpublished by other authors before. As stated by Jeanne M. Liedtka, *"the personal interview has long been recognised as one of the primary methods of pursuing research in social sciences."* (1992:161) In the case of the conducted research, interviews were necessary due to the lack of volume of analyses on the topic of space cybersecurity, as well as regulations and policies which date before the year 2016. The valuable insight that professionals from the field were willing to provide for the purpose of this research may fill the research gap from a security studies point of view.

The research interviews were conducted as semi-structured, though the interviews were more on the structured side, with 7 main interview questions [appendix 2] which were sent to the participants prior to the meeting. One of the research interviews followed an unstructured format in response to the participant's direct request. The researcher would ask for clarification or for additional information on topics that the participants were able to give a particularly valuable report on during the interviews. This ensured that the researcher could obtain relevant information from the participants, while still keeping the interviews within a given timeframe without the need to contact the same participants for further clarifications of newly raised topics. The use of semi-structured interviews results in a combination of positives of the structured interview, where according to Atkinson (2017), the researcher can *"compare and contrast the answers that are given from one interview to the next, so as to construct a complete and rich picture of the subject at hand,"* (Atkinson, 2017) which may be too complicated to do in the case of unstructured interviews.

Some sources call the type of interviewing method used the 'structured open-ended interview', where the wording of questions remains the same for every participant and all the questions are asked in the same order. The questions are formulated in a manner that allows for the interviewee to explain their answer in as much detail as possible. The structured open-ended interview also allows for the researcher to ask any follow-up questions for clarification, as had been done in this research. (Turner III., 2010:756)

Nonetheless, this type of research does not require unstructured interviews, as the researcher does not aim to build rapport with the participants, nor does the research aim for lengthy or long-term cooperation with the participants on the research matter in order to answer the set research questions. The role of the researcher/interviewer in the conducted research interviews is more in the role of a 'detached scientist', which allows for a more structured and less personal approach, which is not required due to the nature of research. (Liedtka, 1992)

4.2.2 Selection of Participants

Given the topic of the thesis, participants with experience in the highly specific field of space cybersecurity had to be contacted for the research interviews. Due to the EU space programme being at the centre point of this thesis, the selected participants had to have thorough knowledge of the EU space programme itself, as well as international and regional cooperation between the EU space programme and other actors. The sample size for this research was very limited, as may be the case with qualitative research. The participants were selected on the basis of whether they would fall under intensive or *"information-rich cases.*" (Bradley, 1993:440) All respondents had to fall under the following categories:

- *Currently working in a position directly related to the area of space cybersecurity*
- *Must have at least four years of professional experience in the field of space cybersecurity*
- *Experience with or knowledge of the EU space programme*

Though the sample was limited, the researcher put care into picking out participants from different public or private entities to ensure obtaining well-rounded responses from different points of view on the issue. All participants were academically and/or professionally active in the field of space cybersecurity in order to give valuable insight into the researched topic.

Participants were chosen from the European Space Policy Institute (ESPI) and the European Union Agency for the Space Programme (EUSPA), as well as private companies CGI (Consultants to Governments and Industry) IT Czech Republic s.r.o., CYSEC and the international affairs think-tank Chatham House. These companies and institutions were chosen specifically for their involvement in the area of space cybersecurity, as well as the EU space programme as a whole, where EUSPA figures as the most relevant 'gatekeeper' of security of the EU space programme, ESPI is a think-tank focusing on European space policies, and CGI IT Czech Republic s.r.o. is a private company, figuring as the largest Czech supplier of space security products to the EUSPA, with CYSEC being a relevant Swiss supplier of such to the ESA. A participant from think-tank Chatham House adds valuable insight to existing policy and strategic foresight, as well as providing a thorough geopolitical background to the issue of space cybersecurity.

4.2.3 Data Processing, Analysis, and Evaluation

Each interview consisted of the researcher and the participant in one single one-on-one interview either in person, through an online meeting platform, or through email, according to the participant's availability. The interviews lasted from 9 minutes to 75 minutes, according to the information the participants were willing to share for the purpose of this research. Each interview was audio-recorded on the researcher's recording device and transcribed in the following days and the audio-recording was thereafter deleted. The transcript was then edited grammatically, as well as to delete any abundant filler words or sounds. The edited and reviewed transcripts were later sent to participants for evaluation, giving them an opportunity to correct their responses, add more information, or delete information they would not wish to be published.

To ensure proper analysis of the research interview transcript, each separate answer was inspected for key information important for the purpose of the research. To do this, qualitative content analysis was used to identify recurring themes and topics. Identification, or coding, of topics and themes in interviews helps to classify information into groups, which allow for better understanding of the researched topic. (Atkinson, 2017:84) Some information was clearly identifiable right away while other, less obvious pieces of information, had to be further researched to help reach the objective of this research. Bogdan and Taylor describe the indicated content analysis method as *"a process which entails an effort to identify formal themes and to construct hypotheses (ideas) as they are suggested by the data and an attempt to demonstrate support for those themes and hypotheses."* (1975:79) Qualitative content analysis is an appropriate data analysis method for this type of research because the search for recurring topics and themes may reveal answers to the research questions that may not be found elsewhere. The hypotheses that the researcher forms throughout the analysis may support the initial hypotheses, thus further supporting the results of the research answering the set research questions. The hypotheses are stated as followed:

H1: *There will be a noticeable increase in cyber-attacks aimed at the EU space programme. Furthermore, the EU will have started forming a coherent response to these.*

H2: *The more frequent and severe cyber threats become to the EU space programme, the greater the regional and international cooperation to mitigate cyber threats.*

The information obtained from the interviews will be supplemented with literature research using both primary and secondary sources. Official EU documents, such as the establishing document of the EUSPA, EU directives and regulations to the EU space programme, analyses by think-tanks and policy institutes, and academic journal articles will be used as sources for the analysis of the historical and current state of cybersecurity of the EU space programme. Furthermore, the development of cooperation between the EU space programme at a regional and international level, as well as cooperation with private companies on the matter of space cybersecurity will be studied. To supplement the existing literature, the researcher aims to obtain information also from space cybersecurity conferences or events which are available online.

Essentially, the thorough study of the transcripts along with relevant literature should ensure correct categorisation of data into thematic groups, which will be discussed further throughout the practical section of this thesis. Evaluation of data gathered from research interviews can be tricky; even though the researcher prepared ground for thorough objective analysis of the transcripts, there is a possibility of bias on what information would be considered as the most important. The researcher prevented bias by working together with the participants and providing them with the final transcripts to add any other important information. Furthermore, there is a high level of trust between the researcher and the participants of the study to be told truthful answers to the interview questions.

4.2.4 Research Limitations

The author of this thesis attempted, to the best of her abilities, to contact participants well in advance in order to create enough space to conduct all the necessary interviews needed for successful completion. However, due to various possible reasons, many of the contacted participants did not reply to the emails sent by the researcher, though they were contacted multiple times. One of the reasons for this could have been that the contacted participants were bound by non-disclosure agreements and knew that the answers they would provide would break the agreement. The lower rate of responses could have also been caused by a lack of trust between the researcher and the possible participants, as the researcher had not been in contact with the participants prior to this research. Though this resulted in a smaller number of interviews than the researcher originally planned, the interviewees were of high relevance to the research and were highly qualified. The researcher attempted to replace some of the information that could have been obtained by watching recordings from conferences on the topic of space cybersecurity, where some of the interview questions were partially answered.

Another possible limitation to this research is the nature of cybersecurity information, where most information about attacks is confidential. Information of this kind, due to its sensitivity and potential to be used with malicious intent, is often only shared among a limited group of people, and not released to the public. Some of the participants disclosed that they have limited knowledge of which types of cyber-attacks are commonly carried out against space systems. Other participants were in possession of this information but were bound to not disclose this information to the public. Private space companies were more open to sharing for example their cybersecurity products, whereas public entities were less forthcoming, especially in terms of technical cybersecurity measures.

Furthermore, throughout the research the researcher realised that in order to create well-rounded research with varying opinions on the matter of space cybersecurity, it would have been helpful to contact persons from other space programmes, to be able to compare the approach of the EU space programme to space cybersecurity to the approaches of different space programmes. This could have created more opportunity to compare and contrast the approaches, as well as giving an insight to how some cybersecurity threats could be handled more effectively. However, due to the scope of this Master's thesis, the comparison of approaches of other national space programmes would exceed the limit of the recommended length; this may create potential avenues for further research.

4.3 Ethical Considerations of Research

The research design for this thesis has been approved by the Charles University Research Ethics Committee of the Faculty of Social Science *[appendix 1]*.

Qualitative research methods often require an ethics committee approval to determine whether the research design is ethical. This particular research has few ethical aspects that need to be taken into consideration, as working with participants has its specifics. There are principles of ethical conduct, which usually encompass anonymity, confidentiality, informed consent, harm, and voluntary participation, among others, depending on the nature of the conducted research. (Lichtman, 2013) Care was put into ensuring that each step of the research process was ethical, the following information will introduce the preparation and process which ensured ethical treatment of participants during research interviews.

The participants were contacted through email, through searchable and publicly available email addresses, or through LinkedIn, after thorough investigation regarding their professional focus. Each participant had a choice whether to participate in the thesis research, so all interviewees participated voluntarily. An informed consent form *[appendix 2 & 3]* was sent to the participants via email prior to the interview for thorough inspection, in either the Czech or English language, and the interview was only conducted after the discussion and signature of the informed consent form. In the case of an interview through email, the participants were sent the consent form together with the interview questions. Understanding the research purpose and the use of the provided information within this thesis was confirmed both through communication and by signing the informed consent form. Interview questions *[appendix 4]* were sent to the participants prior to the interview, so they could either prepare their responses, or choose not to answer certain questions. The participants were given an opt-out option if they did not want their responses to be taken into consideration in this thesis; they had been given three days to withdraw from the research altogether, or they were given the option to delete some of the information stated in the interview from the transcript.

Regarding anonymity and confidentiality, throughout this research special care was taken to ensure these to the highest level possible. Anonymity cannot be ensured completely because the email addresses and names were publicly available before the research, which could potentially lead to de-anonymisation. Confidentiality from the side of the researcher has been maintained; the names of the participants have been omitted from all interviews, audio-recordings of the interviews have been deleted and were only stored on a single device used by the researcher throughout the research. Transcripts were taken by the researcher solely, they were not transcribed using artificial intelligence (AI), transcription services, or third-party individuals. Within this thesis, only the professional affiliation will be stated, agreed upon by the participants, to differentiate between interviews and points of view on the issue of space cybersecurity. With consent of the participants, the reviewed transcripts will be used throughout the thesis.

5. THEMATIC ANALYSIS OF RESEARCH INTERVIEWS

This chapter will discuss mainly the information gained from conducting research interviews with chosen participants from the field of space cybersecurity. Personal, first-hand experience with the EU space programme and the issue of space cybersecurity gives insight foremostly in the current state of the topic, but also into the possibilities of future development in resolving the issue. The opportunities and possible means for the development of further cooperation, both regional and international, as well as between public and private entities will be discussed below.

The structure of the analytical section follows predominantly the structure of the interviews. Firstly, the geopolitical context is discussed, to give an overview of the importance of the issue of EU space programme cybersecurity. Further, the development of cyber threats is discussed, along with the segments most affected. The key identified weaknesses are discussed in detail, and in addition, the political and technical cybersecurity measures, and established policies. Moreover, cooperation in the area of space cybersecurity will be discussed at both a regional level and an international level. Lastly, the current state of public-private cooperation on the researched topic of EU space programme cybersecurity will be explained.

5.1 Geopolitical Background

The space sector is highly important for society; globally, many governments, institutions, and companies, from the financial sector to the energy sector, somewhat rely on space-enabled services. This puts space into a strategic position, and other countries may abuse this. The current geopolitical situation is quite complex, which is why it is important to explain the geopolitical context to the necessity of securing the EU space programme. The current interplay between China and Russia, amidst the war in Ukraine, is particularly worrying.

The geopolitical context was explained, in detail, by the Chatham House participant. The contrast, particularly between the approaches of China and the U.S., was described as the following: *"You have the Western side, the American side, where there's an industrial military complex wanting to go around the world, imposing themselves militarily as a hegemony,"* whereas *"Xi is on a different trajectory. My analysis is that China is on an economic quest for hegemony. China is trying to win it by trade."* (Chatham House participant, 2023) The trajectory that China is on enables it to gain a substantial amount without the need for military force. However, this 'non-military' position must be maintained, or the strategic 'upper hand' with the U.S. could be lost. Which means that China is very unlikely to help Russia in its war on Ukraine militarily - *"they can't send troops to Ukraine. That would just be escalatory."* (Chatham House participant, 2023) Nonetheless, as the participant explains further, *"they probably supplied intelligence already for Russia from Chinese satellites*." (Chatham House participant, 2023)

There are other means than military that China may use to help Russia in maintaining their current position within international relations. As stated by the participant, *"China's options in terms of how Xi can help Putin, and one of the instruments that, in history, goes back to 2010, is when Japan arrested a Chinese trawler in the seven-dash line around the South China Sea… They took it into harbour and China said, 'OK unless you release that trawler, we are going to stop your supplies of silicon', which they did and about a week later the trawler was released with all the 'Sorry about this misunderstanding'."* (Chatham House participant, 2023) China is the leading player in refining and supplying critical minerals globally, refining *"68% of nickel globally, 40% of copper, 59% of lithium, and 73% of cobalt,"* (Castillo & Purdy, 2022) and it understands the leverage that flows from this. It is a leverage that China is willing to administer to countries or companies not in accordance with its objectives, the Chatham House participant gives the example of Lockheed Martin. The issue for the EU space programme is that "our space, satellites, our ground stations, and everything, that consumes an awful lot of critical minerals," (Chatham House participant, 2023) which puts EU space at a significant disadvantage.

However, it is not only the EU space programme which is at a disadvantage; the U.S. and its large commercial space industry and space systems are just as, if not more, vulnerable. Due to the military nature of the U.S. hegemony, as discussed above, that *"the [military] communications required expanded so much that they'll be offloaded from the military systems."* (Chatham House participant, 2023) These communications have to be offloaded onto commercial space objects, which are significantly less secure. It also means that *"there will be linkages between the two," which leads to the question posed by the interviewee: "is there a pathway to get back into the military system through the current commercial systems that you have co-opted?"* (Chatham House participant, 2023) The issues here mentioned may lead to more future insecurity, if not properly handled.

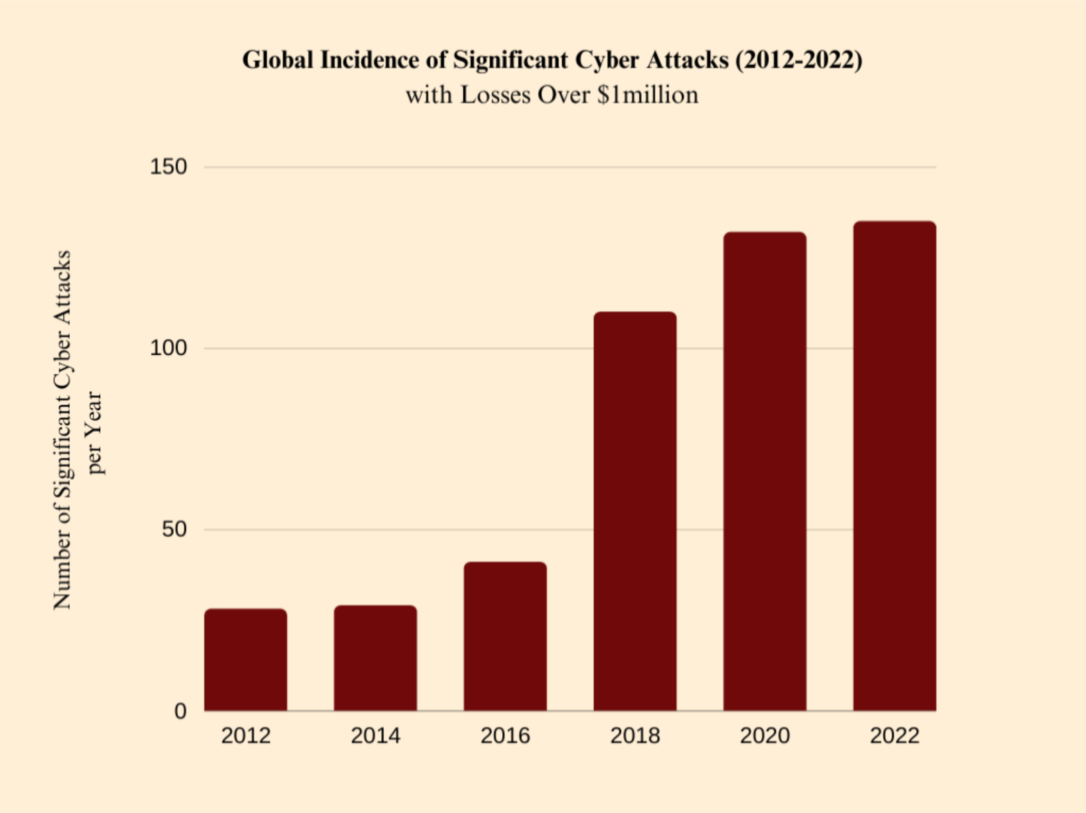
Purely in terms of cybersecurity, the Chatham House participant leads with an illustration of China's cyber capacities, stating that the UK has been *"on a cyber security path for about a decade, since the formation of the National Cybersecurity Centre,"* and currently *"has 7000 or 8000 cyber attackers, and China has got 130,000 cyber attackers."* (Chatham House participant, 2023) A clear imbalance can be seen when comparing the capacities of the U.K. and China, which is alarming. Cyber threats can cause great financial damage, while being relatively cheap; *"these attacks can be executed with relatively low resources and can be contracted out, making them accessible to various state or non-state actors."* (Chatham House participant, 2023) Another issue with cyber-attacks on the space sector infrastructure is attribution. As discussed by the EUSPA participant, *"attribution of cyberattacks remains challenging due to the various methods attackers use to conceal their identities."* (EUSPA participant, 2023) This is further explained by another participant, *"it's a very mobile market and it's very difficult to pin people down."* (Chatham House participant, 2023)

According to the Chatham House participant, *"European Space, and this is not individual to European Space, is we've got this relatively un-manoeuvrable big entity*." (Chatham House participant, 2023) This is further explained: *"it's all about the speed of change, because if you can work faster than the enemy, which is probably unlikely, but if you work faster... this is how in military philosophy, it's how you generate combat power out of an inferior force. You just work faster. And pace is actually the key element here, so whatever is in place has to be configured."* (Chatham House participant, 2023) The need for a higher pace is clear, when observing the offensive cyber capacities that both China and Russia possess, there is a sizable *"mismatch in the pace of events that China or Russia is able to generate in a month."* (Chatham House participant, 2023)

Focusing on the EU space programme and its position in the complex current geopolitical situation, it is vital to acknowledge that *"cyber is a part of the battle,"* (Chatham House participant, 2023) and therefore it is necessary to secure it as much as possible from external interference, be it from China, Russia, or a different actor. This is further supported by an article on cyber-attacks being used as a political threat: *"using cyber-attacks for political reasons is not a new phenomenon."* (Peeters, 2022) The possible consequences that a cyber-attack can have on the EU was showcased in the KA-SAT attack in Ukraine in 2022, where it became clear that *"an attack on a system in Ukraine could then have ripple effects in the UK, Italy, France, Poland… ."* (ESPI participant, 2023) Cybersecurity is a growing issue, and there are consequences when this issue remains unnoticed or mismanaged. However, due to the fragmentation of the EU space programme, an increased collective effort to act in unison, or the vulnerabilities could be exploited.

5.2 A Decade in Cyber Threats

Over the course of the past decade, cyber threats have gained in both strength and number; a serious issue many sectors have observed, including the space sector. The growing number of cyber-attacks in general, not specifically to the EU space programme, can be illustrated through the graph below:



Source: author's own graph. Statistics are from CSIS. https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

The research interview participants generally agreed about the growth of cyber-attacks; *"the EU Space Programme has been perceiving the growth in cyber-attacks in the past decade,"* (EUSPA participant, 2023) the CGI IT participant concurred, as did the ESPI and Chatham house participants. One of the participants continued by stating that *"cybersecurity tends to get forgotten,"* especially when it comes to companies which do not want to invest some of their income into cybersecurity. The CYSEC participant refrained from answering the question due to the lack of publicly available information about this issue.

Regarding the question on the most frequently used type of attack on the EU space programme, the ESPI participant states that *"it is hard to say because we see a lot, and also because it's cyber, there is a lot of information that is not public."* (ESPI participant, 2023) The lack of publicly available information on this topic, due to its sensitive nature, unfortunately resulted in a lack of relevant answers. However, from personal experiences, the CGI IT participant submitted his view on the growing number of cyber threats to the EU space programme by saying *"I am aware of attacks which are used on the tolling systems used in GNSS technologies and these attacks are typical ones - it's not done to destroy the system or to somehow attack the system, but to avoid the duty of paying the toll."* (CGI IT participant, 2023) Furthermore, they explain that, though this is not as common as the previous example, *"attackers may also use spoofing to give the receiver wrong information about the governed position."* (CGI IT participant, 2023) Moreover, they add that *"the Galileo programme and the positioning and timing services are more sensitive to cyber-attacks than for example the Copernicus programme and the EO data,"* (CGI IT participant, 2023) due to their strategic importance for the EU.

Especially during the past few years, there have been efforts to counter the growing number of cyber threats within the EU space programme. According to the ESPI participant, within *“the regulation that established the EU space programme and EUSPA, you have a lot of provisions that mention cybersecurity and security in general,”* (ESPI participant, 2023) which is a very positive step forwards in maintaining a cyber-secure EU space environment. Nonetheless, there are issues and vulnerabilities within the EU space programme, as discussed with other participants, which remain unchecked and may cause problems in the future. For example, the Chatham House participant explains that it would be necessary for EU space to *“do a back order saying which ones are the vulnerable satellites, the up and down links and indeed the ground stations, including the dishes, which ones in the light of this new this new world that we're confronting - which ones have we overlooked the cybersecurity 10 years ago, that we haven't put the right investment in and therefore we've made ourselves open?”* (Chatham House participant, 2023)

Additionally, in order to efficiently counter cyber threats to the EU space programme, both technical and political cybersecurity measures must be employed. As explained by the EUSPA participant, *“while political approaches aim to create an environment where cyber threats are minimised and cooperation is sought with different entities and institutions, the technical ones focus on minimising the identified vulnerability and keeping pace with the technological development of the systems.”* (EUSPA participant, 2023) This is further supported by another participant who concurs that these measures go hand in hand in order to have the desired effect in such a fast-changing environment. (GCI IT participant, 2023)

5.3 The (Decreasingly) Hostile Orbital Systems

When describing the differences between attacks on non-orbital systems, for example on the ground segment, and cyber-attacks generally on another sector, most participants were in accordance with each other. Participants discuss that *"there is not necessarily a big difference between a cyber-attack on a normal computer and, for example, a cyber-attack on a ground station, or on the control segment,"* (ESPI participant, 2023) or that the ground segment *"is very much standard IT - so you have a cloud service, you have servers, you have connectivity on the ground, fibre optics, you have software running on these servers or on these cloud services, mission control, computers, laptops."* (CYSEC participant, 2023) So, there are few differences between cyber-attacks on ground systems of the EU space programme. There are, however, differences between cyber-attacks on non-orbital systems and those executed (or attempted) on orbital systems.

According to the ESPI participant, the difference is with *"cyber-attacks on the satellite itself - on the space segment - when it is in orbit, because then you have the constraints of the orbital environment, which is naturally hostile and very different."* (ESPI participant, 2023) Furthermore, they explain that *"the hostility of the orbital environment, and how far the satellites are from the Earth, can have an impact on encryption, on cybersecurity measures, because usually, traditional cybersecurity measures are implemented."* (ESPI participant, 2023) Additionally, the traditional cybersecurity measures may actually prove to be not entirely functional, since the measures are not adapted for the environment satellites are in, and this may undoubtedly create issues in the future, if left unprovisioned.

The past decade has changed many people's viewpoint on the cybersecurity of the EU space programme, and on the cybersecurity of the space domain overall. Satellites used to be less commercial and more for military uses, which also meant that the ground stations and the command centres were under a higher degree of general security. The orbital segment seemed connected to such a small extent that it was not deemed necessary to have the orbital objects sufficiently secure from cyber interference. However, as the ESPI participant explains, you can currently observe a partial merge of space and cyberspace; *"satellites are increasingly digitalised, they have an increasing number of software components, some of them are powered with IP protocols, so they are technically part of the internet."* (ESPI participant, 2023) The CYSEC participant concurred this information by stating that though *"you are operating an object that is orbiting at 500 or 36 000 km above your head, which seems to be far, but this object is still connected."* (CYSEC participant, 2023)

Nevertheless, one of the participants further added that, when talking about cyber-attacks, *"when the satellite is in orbit, the only way to attack it or to do some damage to the satellite is through the ground segment."* (CYSEC participant, 2023) So far, the orbital segment is still more hostile and less prone to cyber interferences than the ground segment for example, however, the interconnectedness is advancing at a rapid rate, and the security of space-based assets should not be overlooked. The greater the utility of space will be, the more interconnected, the more vulnerable it can become. From the point of view of the Chatham House participant, *"Space will fix it!" Yeah, but - have you gone back to the 4th level of the supply chain? I think people are very glossy if that makes sense."* (Chatham House participant, 2023)

5.4 The Weakest Link

5.4.1 The Supply Chains

The supply chain has been identified as a weak point of the space industry in general. It has also been stated within the EU Space Strategy for Security and Defence, that *"the space sector and its supply-chains are vulnerable to interference."* (European Commission, 2023) A participant stated that *"a lot of the attacks exploited supply chains, not only physical components, but also software components."* (ESPI participant, 2023) Moreover, due to the lack of critical minerals, chip factories, and other necessary components to create satellites or other unique technologies in the EU, and contributing countries to the EU space programme, the supply chain must be internationalised. This is further supported by the ESPI participant, who adds that *"even if you are a start-up, you have an internationalised supply chain, because of the small components, the micro-processors, the semiconductors, they all come from around the world, so you have no choice."* (ESPI participant, 2023)

The issues with a complex and internationalised supply chain stem from the lack of regulation that can be enforced in countries, which do not fall under the EU jurisdiction, or are not obliged, or monitored enough to manufacture products under EU standards. For example, the ESPI participant explains that *"because supply chains are so globalised, there are so many companies and subcontractors, in different countries, and different jurisdictions, different rules, different obligations, it is very difficult to secure."* (ESPI participant, 2023) The participant raises some interesting questions: *"how do you protect against cyber threats during the development of the programme, when satellites are being manufactured by contractors? How do you secure that?"* (ESPI participant, 2023)

The protection of the manufacturing process is also becoming more challenging as *“the need to guarantee high production rates (e.g., 4 satellites per day in the case of the densest constellations) requires the system integrators to stretch globally the existing supply chain, and to include new components providers.”* (Zatti, 2017:8) Moreover, *“manufacturers and developers of space systems may not yet have reached the same level of cyber hardness as other sectors,”* (Weeden & Samson, 2020:17) because the parts that are manufactured may not be vulnerable if used in a different setting, but if integrated into a satellite for example, could be exploited.

The issues with the cybersecurity of the supply chain does not only lie in the problems in jurisdiction, but also in the standards of the manufacturers themselves. For instance, the Chatham House participant argues whether anyone from the EU space programme *“investigated their supply chain all the way down to see if they've cyber vulnerabilities inside their supply chain,”* (Chatham House participant, 2023) because if there is no personal investigation, the likelihood of finding vulnerabilities, or mismanaged manufacturing practices, is very low. Furthermore, the participant appeals to human nature; *“this is your source of profit, this is your life passion, this is what you've invested in, and you discover a vulnerability from way back, when it was TRL 2. Are you actually going to declare?”* (Chatham House participant, 2023)

5.4.2 The User Segment

The next identified vulnerability happens to be *“the user segment, or user terminals, so modems that people have at home, or that end users are using. This is usually very badly protected.”* (ESPI participant, 2023) This is further explained by the participant as being due to the user technologies being quite cheap and replaceable. Although cybersecurity professionals announce vulnerabilities that need patching, operators frequently neglect the cybersecurity of the terminals, without realising that *"it can affect the entire space system, the entire infrastructure."* (ESPI participant, 2023) The KA-SAT attack in Ukraine at the beginning of the war *"created a wake-up call,"* so *"now there is more awareness from satellite operators."* (ESPI participant, 2023)

Additionally, though an operator may be skilled and well-versed in cybersecurity, there are still ways in which attackers may penetrate the security in place. The CYSEC participant explains that, when operating a space-based object, if the operator has *"access to the data and the information it is collecting, so does the potential attacker."* (CYSEC participant, 2023) Furthermore, what makes the user segment vulnerable to cyber-attacks is not only due to unsatisfactory security from external cyber-attacks, but the 'attack' may be administered from within. For example, the Chatham House participants shared a personal story, where an Australian telecommunications company became unavailable after *"a technician in Perth did something, and it introduced some kind of bug, and the whole thing collapsed."* (Chatham House participant, 2023) The participant then continued, saying that *"most often, it's not the mid-range, it's the big [businesses] that say, 'we've got an IT department, the one there - in the basement',"* (Chatham House participant, 2023) when being confronted about their administered cybersecurity measures.

5.4.3 The Development Phase

One of the participants also pointed out the vulnerability of the entire development process of orbital assets; *"all the development phases, from day one in the design phase all* *the way to the launch, when the satellite is actually sitting on the launchpad and waiting to go, this is all very sensitive in potential attack scenarios. We have seen this during testing, during assembly, during development… you name it. All these phases on ground, they are all potential attack scenarios."* (CYSEC participant, 2023) Though this issue is also connected in part to the need for an internationalised supply chain, there are other vulnerabilities present, which can be exploited. Potential vulnerabilities in all the development phases include not only external threats, but also internal malicious actors, or even simple mistakes of employees which in result lead to malfunctions or damage to the object.

5.5 To Prevent or to React?

When asked about whether the EU space programme has a more preventive or reactive space cybersecurity policy, the majority of the participants agreed that both a preventive and a reactive approach is needed in order to achieve sufficient results. According to the EUSPA participant, *"both prevention and reaction are important. Identifying potential vulnerabilities and addressing them proactively is as important as responding to incidents as they occur."* (EUSPA participant, 2023) This claim is further supported by the CGI participant, who explains that *"prevention is key, but of course to be able to react with mitigating the risk of damages is also very, very important."* (CGI participant, 2023)

The ESPI participant also agreed that there are attempts to have both a reactive and a preventive approach, stating that *"policy-wise, it's more reactive, but for the EU space programme I think that in the past few years they really tried to be more preventive and increase the security overall."* (ESPI participant, 2023) They further explain that there is a difference in approach varying from different EU flagship programmes; *"when it comes to the cybersecurity of Galileo for instance, then I would say more preventive, because there is increased encryption etc., so then I would say preventive, but in terms of EU cybersecurity policies, I would say more reactive."* (ESPI participant, 2023)

However, though there is consensus between the participants about the combined use of a preventive and reactive space cybersecurity policy, one of the participants pointed out that *"a lot of the acknowledgements of cyber threats on space systems are just that - acknowledgements,"* (ESPI participant, 2023) and though there is greater progress policy-wise, on the topic of space cybersecurity, the EU may not be fully invested into space cybersecurity as would be appropriate, since it is a rapidly emerging issue. They explain this issue by stating that the EU does acknowledge the problem, but in terms of action against space cybersecurity threats, *"there are no specific ways in which they want to do it."* (ESPI participant, 2023)

5.6 On Cooperation: A European Space ISAC?

On regional and international cooperation on the issue of the cybersecurity of the EU space programme, the participants had mixed views on its current state. Some viewed the EU space programme as highly cooperative with other countries and their public/private entities, but some viewed the cooperation as having space for improvement. Furthermore, there were some doubts expressed on whether the attribution and retaliation for cyber-attacks on EU space infrastructure should be managed by the EU, or by the member state most directly affected.

Foremostly, efforts have already been taken in space cybersecurity intelligence sharing, starting with the cyber and space communities, as explained by the ESPI participant, since *"the space community and the cyber community did not really interact with each other."* (ESPI participant, 2023) This was the first vital step towards firstly, understanding the issue from both points of view, and secondly, building on a more meaningful regional and international cooperation. This is particularly important for the EU space programme, because *"cybersecurity of space missions is a matter of competitiveness for the European space industry, and, at the same time, is a vital subject for the European Union."* (Zatti, 2017:8) It is important to express that *"national approaches in isolation will do little to mitigate harm already being experienced in space assets,"* (Livingstone & Lewis, 2016:8) which is why cooperation is increasingly significant for the competitiveness of the EU space programme.

Due to some fragmentation within the EU and the EU space programme, *"the cybersecurity of the EU space programme is distributed in many member states."* (ESPI participant, 2023) However, because cybersecurity is a growing threat, and the EU space programme is experiencing this threat, there is more cooperation on the matter than before. As stated by the CGI IT participant, *"all the member states try to be somehow harmonised,"* (CGI IT participant, 2023) which shows that there are efforts, and though, according to the ESPI participant, cybersecurity *"in general is not something that is really addressed,"* they also mention that the EU space programme does foster *"cooperation in other ways."* (ESPI participant, 2023) This may be done for example by having *"comprehensive security frameworks, raising awareness of cyber risks and fostering inter-institutional cooperation,"* (EUSPA participant, 2023) for example through the EU Agency for Cybersecurity (ENISA).

As affirmed by the participant, *"sharing intelligence and best practices enables the EU to identify, assess, and address vulnerabilities more effectively."* (EUSPA participant, 2023)

The EU space sector cooperation was showcased on the example of the Public Regulated Service (PRS). The CGI IT participant explained that *"each member state has their own PRS CPA (Competent PRS Authority), which is somehow the centre of the PRS service within each member state."* (CGI IT participant, 2023) The CPAs then have their rights to state whether PRS will or will not be available for certain entities in their respective states. The participant further explained that *"the representatives of each CPA meet on a regular basis, they regularly discuss [findings] for example with EUSPA, they contribute to the development of the service, so in these terms there is definitely some kind of harmonisation within the entire EU."* (CGI IT participant, 2023) Within this example, each member state retains its sovereignty, but shares important information with EUSPA, or other connecting party, in order to keep the EU space sector secure.

Nevertheless, there were some expressions of doubt amongst the participants, especially in terms of attribution or retaliation in case of a cyberattack on infrastructure of the EU space programme. A participant stated their doubt by saying that *"attribution, retaliation and so on is the job of the government, and it should remain the sole domain of the government, otherwise it would be becoming a little bit of the cyber 'far west'."* (ESPI participant, 2023) Furthermore, the participant was sceptical about the state of current EU cooperation on space cybersecurity, because there can be *"cooperation agreements for cybersecurity between states, but it is very rare that it covers space cybersecurity."* (ESPI participant, 2023) EUSPA's Security Accreditation Board Chair stated, at the 2022 CYSAT conference, that thanks to its *"robust security apparatus, EUSPA is at the front lines of cybersecurity,"* however, cybersecurity within the space programme is mainly delegated to trusted entities, where EUSPA figures as a supervisor to their activity, according to information provided by the interviews.

As explained by Livingstone and Lewis (2016), *"the dialogue on cybersecurity in space cannot be confined to a broad but fragmented approach by individual states and international organisations, albeit each acting in good faith."* (2016:8) Cooperation within the EU is at a relatively high level, due to the oversight of the EUSPA and the EC, but international cooperation is still at a relatively low level, in terms of intelligence sharing on cybersecurity threats to the space sector. However, as explained by the EUSPA participant, *"political approaches, such as promoting international cooperation and the establishment of norms of responsible behaviour in cyberspace, are prerogative of the European Commission."* (EUSPA participant, 2023) This means that in terms of international cooperation, there is one sole institution which manages and oversees it on behalf of the whole EU space programme, which could potentially halt the efforts for greater international cooperation. Furthermore, the EUSPA participant explains that *"collaboration with international partners contributes to the exchange of information, the development of shared standards, and the fostering of a global culture of cyber security."* (EUSPA participant, 2023)

Space ISAC is described as a *"U.S. based organisation for intelligence sharing and risk sharing on cyber threats on space systems. It includes US intelligence agencies and federal agencies, US space companies and some non-US space companies."* (ESPI participant, 2023) The CYSEC participant also mentions Space ISAC as a relevant cooperation platform. However, Space ISAC, in its current state, is apparently dominated by the U.S., which the CYSEC participant views as less than optimal: *"whether it is a good idea to go with the Americans or to try our own ISAC as a European thing is something open* *for debate."* (CYSEC participant, 2023) It is a good question to discuss, whether the EU should keep more closed, to cooperate more regionally, or if there should be more of a global cooperation. As stated by the ESPI participant, *"nothing comparable to space ISAC exists within the EU, but European companies can join Space ISAC."* (ESPI participant, 2023) For this reason, the EU Space Strategy for Security and Defence proposes the creation of an EU Space ISAC, for better and tighter EU space programme cooperation. (European Commission, 2023) The ESPI participant further mentions that *"other Space ISAC are trying to be established elsewhere, it is something that countries increasingly find relevant, also in the EU, some member states are increasingly integrating space into their CERT/CSIRT."* (ESPI participant, 2023) The establishment of a Space ISAC within the EU would be a beneficial step to take in order for the EU space programme to maintain its competitiveness.

Higher levels of cooperation can be attained by other means than the creation of a Space ISAC, however, this may be much more complex. The Chatham House participant mentions the UK space programme as comparison to the EU possibilities of cooperation. They state that *"we have the Five Eyes[2],"* (Chatham House participant, 2023) which is a natural cooperation due to the pack of cultural constraints between the participating countries. They further state that *"it's more difficult for the EU I think, because culturally, we all speak English in Five Eyes, and we've all got sort of fairly common groups."* (Chatham House participant, 2023) On the possibilities of EU cooperation on the matters of space cybersecurity, the Chatham House participant further poses the question *"these are different cultures, different languages, people you've not met before, especially if it's a very big gang of 27 or so - how will you actually end up with that proper personal trust?"* (Chatham House participant, 2023)

[2] An intelligence sharing agreement. A cooperation between countries which used to be a part of the Commonwealth – U.K., U.S., Canada, Australia, and New Zealand.

5.7 Public-Private Cybersecurity Cooperation for a Safer EU Space Programme

According to the ESPI participant, the aforementioned U.S. Space ISAC may be seen as some of the more well-established cooperation platforms in terms of public and private entities, as it *"really puts public and private stakeholders at the same table."* (ESPI participant, 2023) In terms of EU private-public cooperation on space cybersecurity, the participant also mentions that *"there is an increasing number of space cybersecurity companies, which was not the case a few years ago, and of course there is cooperation with public actors to have a better understanding of their needs."* (ESPI participant, 2023)

The growing cooperation between public and private entities has also been described by other participants, for example, the EUSPA participant's point of view is that it is *"deemed essential, as many space technologies and services are provided by private companies."* (EUSPA participant, 2023) A few of the participants mentioned the IRIS² flagship programme as a new initiative on public-private cooperation. (ESPI participant, 2023; CYSEC participant, 2023) The CYSEC participant further noted that *"there is a more pragmatic approach in allowing start-ups to be on board and to develop innovative services and technologies with less heritage in the space industry."* (CYSEC participant, 2023) According to the CYSEC participant, thanks to more public-private cooperation, the IRIS² flagship programme *"is going to try to be as good as Galileo, maybe even more agile, more versatile, more useful in a way for EU citizens and with a better use of the allocated budget."* (CYSEC participant, 2023) This is further supported by another participant stating that *"the objective of the constellation is to be secure enough for government communication and secure communication, so it has to be secure enough for this, but it also has to be flexible* *enough for commercial applications,"* (ESPI participant, 2023) which can be realised mainly through public-private cooperation.

Furthermore, the current state of public-private cooperation in space cybersecurity is shown through the case of CGI IT Czech Republic, as the participant affiliated with this company states: *"there is a deep and long-term collaboration between the public and the private sector… our company is a great example of this. Our company is the biggest Czech supplier with regard to EUSPA, … providing space security-oriented services."* (CGI IT participant, 2023) In addition, the CGI IT participant also disclosed that *"private companies share intelligence on space cybersecurity amongst themselves. Even the core of all the space programmes is based on the knowledge and delivery of the private sector companies."* (CGI IT participant, 2023) Intelligence sharing within the private sector on space cybersecurity issues can lead to faster response time to cyber threats to the EU space programme.

However, there is still room to grow in terms of public-private cooperation, as *"there is very limited public-private cooperation and intelligence sharing on space cybersecurity issues. That is the situation as it is today."* (CYSEC participant, 2023) Additionally, the EUSPA participant stated that *"public-private cooperation in the space sector in terms of intelligence sharing on cyber security threats and vulnerabilities is an emergent field of activity."* (EUSPA participant, 2023) Though the cooperation on space cybersecurity may not be as advanced yet, the EU space programme is striving for more cooperation in the area in the future. Nonetheless, it is still important to acknowledge that *"public/private partnerships create challenges, so it remains to be seen how this will be tackled,"* (ESPI participant, 2023) especially in terms of the supply chain security as discussed earlier.

5.8 The Discussion of Findings

After careful consideration of the information given by the research interview participants, key points were identified, which will be discussed below. Firstly, the geopolitical context to the issue of space cybersecurity as a global issue was discussed. The complex current state of international affairs sets the issue of space cybersecurity at the forefront, as has been illustrated by the damage that cyber-attacks to the EU space infrastructure may have, i.e., the Viasat KA-SAT network attack.

Answering the first research question, *"how have cyber threats to the EU space programme evolved in the past years? How have these threats been addressed within the EU?"*, the key findings of the research interviews were that there has been perceived growth of cyber-attacks to the EU space programme. This finding is particularly important, as it is necessary to acknowledge an issue before there can be any solutions proposed. Furthermore, the analysis of interviews concluded that there are three main weak points within the EU space programme, these being: 1) the internationalised supply chain, 2) the user segment, end-point users, and 3) the insufficient security of the process of development of new technologies. The threats were addressed using a combination of political and technical cybersecurity measures, as well as more sophisticated preventative policies and agile responses to cyber-attacks.

The findings relating to the second research question, "*do threats to the EU space programme from the cyber domain help member states foster regional and international cooperation in order to mitigate said threats?"*, were more dispersed. Cooperation within the EU was generally viewed as more fragmented, though there are increasing attempts within the field of cybersecurity. In terms of international cooperation, the most prominent point was the beneficial prerequisite for successful cooperation - the U.S.-initiated Space ISAC. However, participants saw space for improvement in intelligence sharing on cyber threats to the space sector. The most relevant key finding on regional and international cooperation is the possibility for establishing a European Space ISAC. (European Commission, 2023) Space ISAC is a good platform model, however, due to the time-sensitive nature of cyber-attacks, there should be a smaller, more agile Space ISAC for intelligence sharing amongst solely countries participating in the EU space programme. Lastly, public-private cooperation may indeed be helpful in maintaining a more cyber-secure EU space environment, however, this must be done under a strict regulatory framework set by the EU, for example under the new focus of the NIS 2 (Network and Information Security) directive. (EU Directive 2022/2555, 2022)

Following the above key findings, the research proved both hypotheses stated in the methodological part of this thesis. The first hypothesis stated that *"there will be a noticeable increase in cyber-attacks aimed at the EU space programme. Furthermore, the EU will have started forming a coherent response to these."* The increase of cyber-attacks was proven by the professional and personal experiences provided by the participants, and the response to these is more noticeable. The EU Space Strategy for Security and Defence is one of the necessary steps towards a safer EU space programme from cyber threats. The second hypothesis, in response to the second research question as discussed above, states that *"the more frequent and severe cyber threats become to the EU space programme, the greater the regional and international cooperation to mitigate cyber threats."* The second hypothesis was also accepted and proven, though not in unison as the first hypothesis. The EU has indeed placed ground for a more effective regional cooperation, and international cooperation on the matter of cybersecurity of the EU space programme is also an emergent field. The greatest effort so far is the proposal of the creation of the EU Space ISAC, and hopefully, these efforts will continue in the future.

As has been discussed, there is a growing number of cyber-attacks on the EU space programme infrastructure, and this is becoming more of an issue. With the growth of interconnectedness between space-based assets and other segments of the space programme through the internet, and the space being the single point of failure for multiple sectors, the space sector is necessary to secure. (President's Commission on Critical Infrastructure Protection, 1997:12) There has been a growing number of research papers, analyses, and journal articles on the topic of space cybersecurity, calling for further action. The EU, though not yet fully focused on this issue, has been cooperating more due to the increasing threat of cyber-attacks on the EU space programme. The possibility of the EU space programme to stand against the threat in unison, especially through the creation of a European Space ISAC shows that there is a collective effort for collaborative action. As the threat may proceed even further in the years to come, the need for an even tighter European community will grow too.

It is important to set the findings of the analysis of the conducted research interviews into the theoretical framework of collective identity and identity building through shared threat. As has been discussed above, the threat of insufficient cybersecurity of various weak points of the EU space programme has been proven to become a serious issue, especially in its geopolitical context and the need for an internationalised supply chain. The accountability issue with all cyber-attacks from external malicious actors leads to the 'collective enemy' being a non-identifiable entity. Additionally, the cyber threats may not necessarily come from a state actor or a cyber-criminal gang but may accidently come from a misinformed or under-educated employee or may be caused by lack of governance over, i.e., the supply chain or the development phases of technologies. Therefore, the 'collective enemy' that the EU space programme is facing are the cyber-attacks or exploitations themselves.

Forming around the threat is the collective identity of the EU and the cooperating entities of the EU space programme, to mitigate the effects cyber-attacks are causing to the EU space infrastructure. Identity building around shared threat can be observed within the steps of the EU space programme in mitigating cyber threats. We see that as the threat grows, there is more ambition to cooperate on the topic of space cybersecurity, especially within the EU. The possibility of creation of an EU Space ISAC is a direct response to the rising threats aimed at the European space infrastructure and can be attributed to the cohesion between the member states.

Placing the research interview analysis into context of previous studies on the topic of space cybersecurity, there has been some information, as well as past reflections on possible future development confirmed. However, due to the field of space cybersecurity progressing at such a fast rate that more research is needed constantly, particularly to evaluate and address the current weak points, implement preventive measures, consider policy responses to attempted or successful cyber-attacks, and build strong and long-lasting cooperation. The call for space cybersecurity is slowly becoming acknowledged as a priority for space programmes and providers, including the EU space programme, which is a positive development. Nevertheless, it is important to understand that the field is so susceptible to rapid changes, that a focused, flexible, and agile approach is needed.

6. CONCLUSION

The aim of this thesis was to find out how the cyber threats to the EU space programme have been evolving in the past decade, and how the EU managed to respond to these threats. The research also attempted to create a general overview of the past and current cooperation on the topic of space cybersecurity within the EU and internationally, and how this may have helped the EU space programme in countering cyber threats. This was done through the theoretical framework of collective identity and identity building through shared threat. The research for this thesis was done through analysis of previous research, as well as analysis of conducted research interviews on the topic of EU space programme cybersecurity.

Based on the research interviews, it was found that cyber-attacks on the EU space programme have been increasing in the past decade. The analysis of the interviews identified three main weak points in the EU space programme, namely the internationalized supply chain – an issue which is becoming more prominent with the emergence of New Space, end-point users in the user segment, due to the lack of sufficient user terminal security, and inadequate regulation in the process of development of new technologies. To address these threats, political and technical cybersecurity measures were combined with more advanced preventative and responsive policies. A key point relating to regional and international cooperation on cybersecurity of the EU space programme was the possibility of the creation of a European Space ISAC. This would further aid in making cooperation easier between states, national space programmes, ESA, and private entities within the EU space programme. International cooperation is still emerging; there is still a lot of space for improvement – streamlining cooperation may aid in responding collectively to the fast-evolving threat to cybersecurity of not only the EU space programme, but of space programmes globally.

Moreover, the research hypotheses were both accepted and proven throughout the research for this thesis. There has indeed been a perceived growth in the number of cyber-attacks the EU space programme has been facing over the past decade. Furthermore, the EU, through the establishment of the EUSPA, but also through the EU Space Strategy for Security and Defence, managed to start forming a robust framework dealing with governance and cyber threat mitigation. The second hypothesis has also been accepted; though the research here was not so clearly indicative as when proving the first hypothesis, cooperation in the area of space cybersecurity is an emerging area of focus and will be even more so in the future.

Throughout conducting the research for this thesis, some other research gaps were identified, which open an opportunity for researchers to further research the cybersecurity aspects to the EU space programme. Namely the regulation and standards that are not currently being met by the internationalised supply chain, or the possible threats that arise from the conjoining of military and commercial space-based asset

Summary

Globally, cyber-attacks have been on the rise over the past decade, and the EU space programme is not exempt to these. Due to many European industries and sectors relying heavily on space-enabled systems, maintaining the security and availability of EU space is key for the proper function and prosperity of the EU. With the emergence of New Space, space-based systems are becoming more connected to the internet, creating more vulnerabilities which can be exploited by cyber-attackers.

Space cybersecurity has not been on the forefront of researchers' focus until now. The past decade has shown a shift in attention towards the issue of space cybersecurity, but this mainly focuses outside of the EU. This research aims to find out how cyber threats to the EU space programme have evolved throughout the past decade and how they have been tackled within the EU. Regional and international cooperation on the matters of space cybersecurity of the EU space programme will also be explored through the theoretical framework of collective identity and identity building through shared threat.

The research questions for this thesis were: 1. *How have cyber threats to the EU space programme evolved in the past years? How have these threats been addressed within the EU?* and *2. Do threats to the EU space programme from the cyber domain help member states foster regional and international cooperation in order to mitigate said threats?*

The hypotheses for the research outcomes were: 1. *there will be a noticeable increase in cyber-attacks aimed at the EU space programme. Furthermore, the EU will have started forming a coherent response to these,* and 2. *the more frequent and severe cyber threats become to the EU space programme, the greater the regional and international cooperation to mitigate cyber threats.*

The research for this thesis was done through the study of available literature, official EU communications and conducting research interviews with chosen experts in the field of space cybersecurity. The interviews with experts from the field shed light on the current situation, geopolitical significance, and possibilities for cooperation for a more secure EU space

programme. Finally, this thesis will discuss key findings of the thematic analysis of research interviews and studied literature, which may help in the future development of cooperation in securing the EU space programme from cyber threats.

Based on the research interviews, it was found that cyber-attacks on the EU space programme have been increasing in the past decade. The analysis of the interviews identified three main weak points in the EU space programme, 1) the internationalized supply chain – an issue which is becoming more prominent with the emergence of New Space, 2) end-point users in the user segment, due to the lack of sufficient user terminal security, and 3) inadequate regulation in the process of development of new technologies. To address these threats, political and technical cybersecurity measures were combined with more advanced preventative and responsive policies. A key point attained from the research interviews on regional and international cooperation on the issue of cybersecurity of the EU space programme was the possibility of the creation of a European Space ISAC. International cooperation is still emerging; there is still a lot of space for improvement – streamlining cooperation may aid in responding collectively to the fast-evolving threat to cybersecurity of not only the EU space programme, but of space programmes globally.

The research hypotheses were both accepted and proven throughout the research for this thesis. There has indeed been a perceived growth in the number of cyber-attacks the EU space programme has been facing over the past decade. The EU, through the establishment of the EUSPA, but also through the EU Space Strategy for Security and Defence, managed to start forming a robust framework dealing with governance and cyber threat mitigation. The second hypothesis has also been accepted. Cooperation in the area of space cybersecurity is an emerging area of focus and will be even more so in the future.

Throughout conducting the research for this thesis, some opportunities for further research were identified, i.e., maintaining a high level of cybersecurity within the internationalised supply chain necessary for EU space or the possible threats that arise from using both military and commercial space infrastructure for military purposes.

List of References

Atkinson, J. D. (2017). Qualitative Methods. In *Journey into Social Activism: Qualitative Approaches*. Fordham University Press, 65-98. http://www.jstor.org/stable/j.ctt1hfr0rk.6.

Bailey, B. et al. (2019). Defending Spacecraft in the Cyber Domain. *Aerospace: Center for Space Policy and Strategy*. https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf.

Ball, D., & Waters, G. (2013). Cyber Defence and Warfare. *Security Challenges*, *9*(2), 91–98. http://www.jstor.org/stable/26462919.

Baylon, C. (2014). Challenges at the Intersection of Cyber Security and Space Security: Country and International Institutions Perspective. *Chatham House*. https://www.chathamhouse.org/sites/default/files/field/field_document/20141229CyberSecuritySpaceSecurityBaylonFinal.pdf.

Black, S. (2008). Methods of Interference. In *No Harmful Interference with Space Objects: The Key to Confidence-Building.* 5–8. *Stimson Center*. http://www.jstor.org/stable/resrep10934.6.

Bogdan, R. and Taylor, S. J. (1975). *Introduction to qualitative research methods: a phenomenological approach to the social sciences*. Wiley. ISBN: 978-0-471-08571-3.

Bradley, J. (1993). Methodological Issues and Practices in Qualitative Research. *The Library Quarterly: Information, Community, Policy*, *63*(4), 431–449. http://www.jstor.org/stable/4308865.

Castillo, R. & Purdy, C. (2022). China's Role in Supplying Critical Minerals for the Global Energy Transition. The Brookings Institution. https://www.brookings.edu/wp-content/uploads/2022/08/LTRC_ChinaSupplyChain.pdf.

CCDCOE (2022). Viasat KA-SAT Attack. *The NATO Cooperative Cyber Defence Centre of Excellence.* https://cyberlaw.ccdcoe.org/wiki/Viasat_KA-SAT_attack_(2022).

CERT-EU (2023). Russia's War on Ukraine: One Year of Cyber Operations. https://www.cert.europa.eu/static/threat-intelligence/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf.

Cerqueira, C. S., et al. (2013). Development of an Interface to a Spacecraft Simulator Empowered by Virtual Reality. *SBC Journal on 3D Interactive Systems*. 3. 37-44. DOI: 10.5753/jis.2012.620.

Checkel, J. T. & Katzenstein P. J. (2009). The Politicization of European Identities in European Identity. Cambridge University Press. http://assets.cambridge.org/97805218/83016/excerpt/9780521883016_excerpt.pdf.

Citrin, J. and Sides, J. (2004). Can Europe exist without Europeans? Problems of identity in a multinational community. Advances in Political Psychology 1: 41–70. ISBN: 978-0-080-43989-1.

CSIS (2006-2023). Living document: Significant Cyber Incidents. *Center for Strategic and International Studies.* https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

Cuhadar, E., & Dayton, B. (2011). The Social Psychology of Identity and Intergroup Conflict: From Theory to Practice. *International Studies Perspectives*, *12*(3), 273–293. http://www.jstor.org/stable/44218664.

Eisenstadt, S. N. & Geisen, B. (1995). The Construction of Collective Identity. *European Journal of Sociology*, 36, pp 72-102 doi:10.1017/S0003975600007116.

ESPI (2018). Cyber Security: High Stakes for the Space Sector. *European Space Policy Institute.* https://www.espi.or.at/briefs/cyber-security-high-stakes-for-the-space-sector/.

European Commission (2006). Security Clearance Procedures: Data Protection Notice. *European Data Protection Supervisor*. https://edps.europa.eu/system/files/2022-03/edps_data_protection_notice_security_clearance_procedures_en.pdf.

European Commission (2012). Establishing appropriate relations between the EU and the European Space Agency (COM/2012/0671). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52012DC0671&from=HU.

European Commission (2023). EU Space Strategy for Security and Defence. https://defence-industry-space.ec.europa.eu/system/files/2023-03/EU%20SSSD%20factsheet_1.pdf.

European External Action Service (2022). A Strategic Compass for Security and Defence. https://www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf.

European Parliament (2022). Cybersecurity: Main and Emerging Threats. *European Parliament News.* https://www.europarl.europa.eu/news/en/headlines/society/20220120STO21428/cybersecurity-main-and-emerging-threats.

European Parliament and Council of the EU (2022). EU Directive 2022/2555 on measures for a high common level of cybersecurity across the Union. *Official Journal of the EU.* https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555&qid=1682940284731.

EUSPA (2022). EUSPA: the gatekeeper to a secure EU Space Programme. https://www.euspa.europa.eu/newsroom/news/euspa-gatekeeper-secure-eu-space-programme.

Fidler, D. P. (2018). Cybersecurity and the New Era of Space Activities. *Council on Foreign Relations*. http://www.jstor.org/stable/resrep29932.

Fligstein, N. et al. (2012). European Integration, Nationalism and European Identity. JCMS 2012 Volume 50(1), 106–122. DOI: 10.1111/j.1468-5965.2011.02230.x.

Fouad, N. S. (2021). Securing higher education against cyberthreats: from an institutional risk to a national policy challenge. *Journal of Cyber Policy*, 6:2, 137-154, DOI: 10.1080/23738871.2021.1973526.

Goward, D. (2017). GPS Spoofing Incident Points to Fragility of Navigation Satellites. *National Defense*, *102*(766), 18–19. https://www.jstor.org/stable/27021938.

Hitchens, T., & Goren, N. (2017). *International Cybersecurity Information Sharing Agreements*. Centre for International & Security Studies, University of Maryland. http://www.jstor.org/stable/resrep20426.

Hooghe, L., & Marks, G. (2004). Does Identity or Economic Rationality Drive Public Opinion on European Integration? *PS: Political Science and Politics*, *37*(3), 415–420. http://www.jstor.org/stable/4488854.

Housen-Couriel, D. (2015). Cybersecurity and Anti-Satellite Capabilities (ASAT): New Threats and New Legal Responses. *Journal of Law & Cyber Warfare*, *4*(3), 116–149. http://www.jstor.org/stable/26441259.

Howell, E. (2022). Elon Musk says Russia is ramping up cyberattacks on SpaceX's Starlink systems in Ukraine. *Space.com News*. https://www.space.com/starlink-russian-cyberattacks-ramp-up-efforts-elon-musk.

King, M. & Goguichvili, S. (2020). Cybersecurity Threats in Space: A Roadmap for Future Policy. *Wilson Center*. https://www.wilsoncenter.org/blog-post/cybersecurity-threats-space-roadmap-future-policy.

Khandelwal, S. (2015). Russian Hackers Hijack Satellite to Steal Data from Thousands of Hacked Computers. *The Hacker News*. https://thehackernews.com/2015/09/hacking-satellite.html.

Krasny, M. E. (2020). Identity. In *Advancing Environmental Education Practice*. Cornell University Press, 149–159. http://www.jstor.org/stable/10.7591/j.ctv310vjmw.16.

Libicki, M. C. (2016). Is There a Cybersecurity Dilemma? *The Cyber Defense Review*, *1*(1), 129–140. http://www.jstor.org/stable/26267303.

Lichtman, M. (2013). *Qualitative Research in Education: A User's Guide* (Third edition). Sage Publications. ISBN: 978-1-452-28951-9.

Liedtka, J. M. (1992). Exploring Ethical Issues Using Personal Interviews. *Business Ethics Quarterly*, *2*(2), 161–181. https://doi.org/10.2307/3857569.

Livingstone, D & Lewis, P. (2016). Space, the Final Frontier for Cybersecurity? *Chatham House*. https://www.chathamhouse.org/sites/default/files/publications/research/2016-09-22-space-final-frontier-cybersecurity-livingstone-lewis.pdf.

MacGibbon, A. (2009). Cyber security: threats and responses in the information age. *Australian Strategic Policy Institute*. http://www.jstor.org/stable/resrep03941.

Manulis, M. et al. (2020). Cyber security in New Space: Analysis of Threats, Key Enabling Technologies, and Challenges. *International Journal of Information Security.* https://doi.org/10.1007/s10207-020-00503-w.

Matonytė, I., & Morkevičius, V. (2009). Threat Perception and European Identity Building: The Case of Elites in Belgium, Germany, Lithuania, and Poland. *Europe-Asia Studies*, *61*(6), 967–985. http://www.jstor.org/stable/27752329.

NASA, (2022). Chapter 11: Ground Data Systems and Mission Operations *in* State-of-the-Art Small Spacecraft Technology. https://www.nasa.gov/smallsat-institute/sst-soa/ground-data-systems-and-mission-operations#_Toc121310375.

NATO (2022). NATO's Overarching Space Policy. *North Atlantic Treaty Organisation.* https://www.nato.int/cps/en/natohq/official_texts_190862.htm.

Peeters, W. (2022). Cyberattacks on Satellites: An Underestimated Political Threat. London School of Economics and Political Science. https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites.

Poirier, C. (2022). The War in Ukraine from a Space Cybersecurity Perspective. *European Space Policy Institute.* https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Short-1-Final-Report.pdf.

Porche, I. R., et al. (2013). How Electronic Warfare Overlaps with Other Areas. In *Redefining Information Warfare Boundaries for an Army in a Wireless World*, 43–56. *RAND Corporation.* http://www.jstor.org/stable/10.7249/j.ctt3fh1qp.13.

President's Commission on Critical Infrastructure Protection (1997), *Critical Foundations: Protecting America's Infrastructures*, http://permanent.access.gpo.gov/lps15260/PCCIP_Report.pdf.

Publications Office of the EU (2022). EU Space Programme (2021-2027) - European Union Agency for the Space Programme. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM:4526706.

Rousseau, D. L., & Garcia-Retamero, R. (2007). Identity, Power, and Threat Perception: A Cross-National Experimental Study. *The Journal of Conflict Resolution*, *51*(5), 744–771. http://www.jstor.org/stable/27638576.

Risse-Kappen, T. (1995). Democratic Peace - Warlike Democracies? A Social Constructivist Interpretation of the Liberal Argument. *European Journal of International Relations* 1: 4, 491-517. ISBN: 978-1-315-62366-5.

Risse-Kappen, T. (2010). A Community of Europeans?: Transnational Identities and Public Spheres. Cornell University Press. ISBN 978-0-8014-7648-8.

Santamarta, R. (2018). White Paper: Last Call for SATCOM Security. *IOActive: Research Fuelled Security Services*. https://ioactive.com/wp-content/uploads/2018/08/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf.

Ścigaj, P. (2020). Identity (Including Collective Identity): The History of Reflection, Research Scope and Overview of Definitions. *Politeja*, *68*, 3–33. https://www.jstor.org/stable/27037090.

Shadbolt, L. (2021). Technical Study: Satellite Cyberattacks and Security. HDI Global Specialty SE. https://www.hdi-specialty.com/downloads/_Global/HDIS209_Satellite_Cyberattack_whitepaper.pdf.

Steinberger, J. A. (2008). A Survey of Satellite Communications System Vulnerabilities. *Air Force Institute of Technology*. https://apps.dtic.mil/sti/pdfs/ADA487592.pdf.

Tadjdeh, Y. (2018). Army Merging Electronic Warfare, Cyber Ops. *National Defense*, *102*(771), 7–7. https://www.jstor.org/stable/27022076.

Tajfel, H., & Turner, J. C. (1979). An integrative theory of intergroup conflict. In W. G. Austin, & S. Worchel (Eds.), The social psychology of intergroup relations (pp. 33-37). Monterey, CA: Brooks/Cole. ISBN: 978-0-818-50278-1.

Thales (2023). Thales Seizes Control of ESA Demonstration Satellite in First Cybersecurity Exercise of its Kind. Thales Group. https://www.thalesgroup.com/en/worldwide/security/press_release/thales-seizes-control-esa-demonstration-satellite-first.

Theohary, C. A. & Hoehn, J. R. (2019). Convergence of Cyberspace Operations and Electronic Warfare. *Congressional Research Service.* https://sgp.fas.org/crs/natsec/IF11292.pdf.

Toukebri, R. (2021). Cybersecurity Risk Mitigation for Ground Systems. *Space Generation Advisory Council.* https://spacegeneration.org/cybersecurity-risk-mitigation.

Turner III., D. W. (2010). Qualitative Interview Design: A Practical Guide for Novice Investigators. The Qualitative Report, 15(3), 754-760. https://doi.org/10.46743/2160-3715/2010.1178.

Weeden, B. & Samson, V. (2020). Global Counterspace Capabilities: An Open Source Assessment. *Secure World Foundation*. https://swfound.org/media/206957/swf_global_counterspace_april2020_es.pdf.

Wendt, A. (1994). Collective Identity Formation and the International State. *The American Political Science Review*, *88*(2), 384–396. https://doi.org/10.2307/2944711.

Westbrook, T. (2019). The Global Positioning System and Military Jamming: geographies of electronic warfare. *Journal of Strategic Security*, *12*(2), 1–16. https://www.jstor.org/stable/26696257.

Zatti, S. (2017). The Protection of Space Missions: Threats and Cyber Threats. In: Shyamasundar, R., Singh, V., Vaidya, J. (eds) Information Systems Security. ICISS 2017. Springer. https://doi.org/10.1007/978-3-319-72598-7_1.

Zielinski, R. H., et al. (1996). Star Tek - Exploiting the Final Frontier: Counterspace Operations in 2025. *Defence Technical Information Center*. https://apps.dtic.mil/sti/citations/ADA392588.

Research Interviews:

ESPI participant (2023). Research Interview: Tackling Cybersecurity Threats to the EU Space Programme: Regional and International Cooperation. Appendix 5.

EUSPA participant (2023). Research Interview: Tackling Cybersecurity Threats to the EU Space Programme: Regional and International Cooperation. Appendix 6.

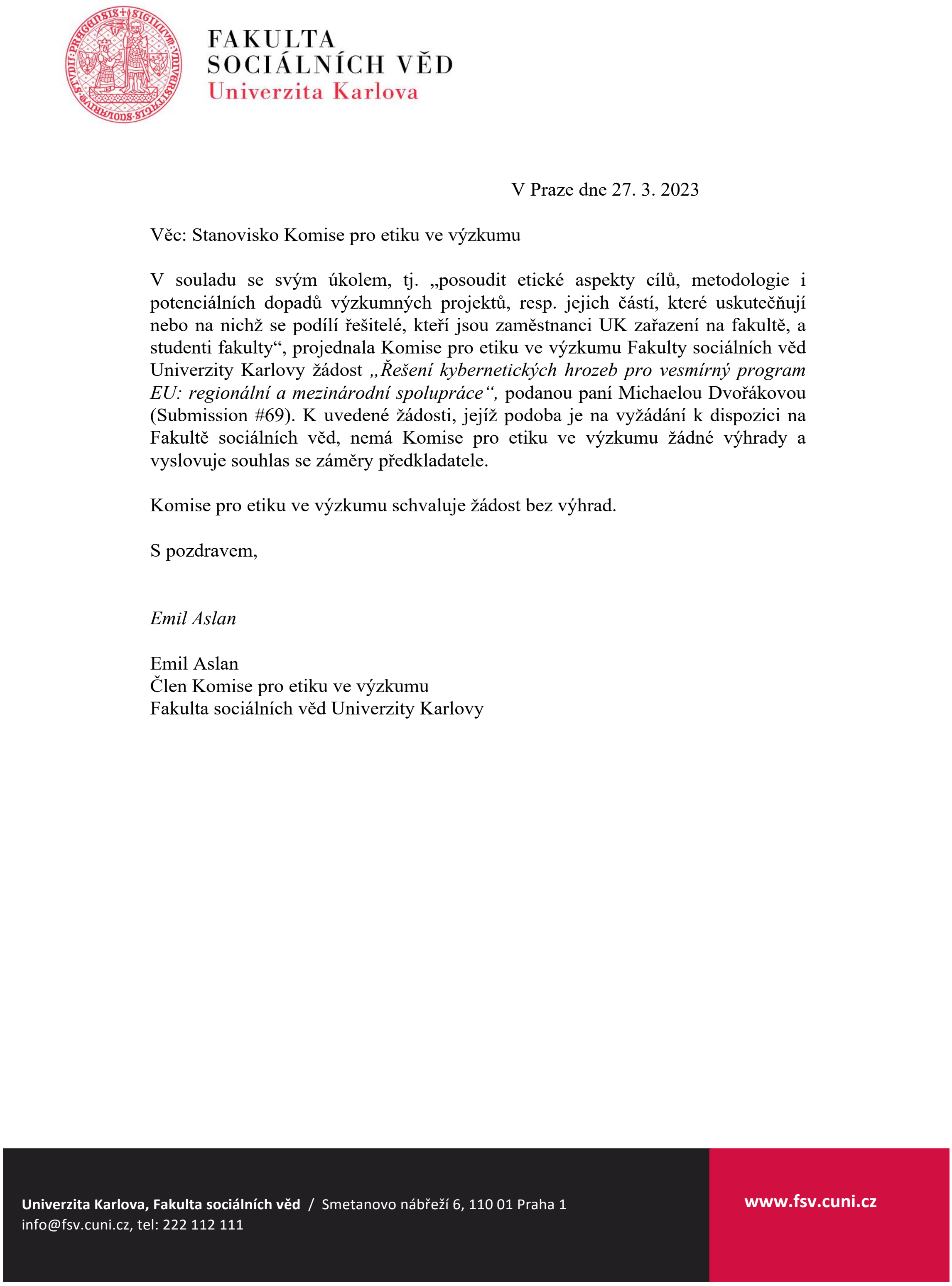
CGI IT Czech Republic participant (2023). Research Interview: Tackling Cybersecurity Threats to the EU Space Programme: Regional and International Cooperation. Appendix 7.

CYSEC participant (2023). Research Interview: Tackling Cybersecurity Threats to the EU Space Programme: Regional and International Cooperation. Appendix 8.

Chatham House participant (2023). Research Interview: Tackling Cybersecurity Threats to the EU Space Programme: Regional and International Cooperation. Appendix 9.

List of Appendices

Appendix no. 1: Charles University Research Ethics Committee - Research Ethics Approval



FAKULTA
SOCIÁLNÍCH VĚD
Univerzita Karlova

V Praze dne 27. 3. 2023

Věc: Stanovisko Komise pro etiku ve výzkumu

V souladu se svým úkolem, tj. „posoudit etické aspekty cílů, metodologie i potenciálních dopadů výzkumných projektů, resp. jejich částí, které uskutečňují nebo na nichž se podílí řešitelé, kteří jsou zaměstnanci UK zařazení na fakultě, a studenti fakulty“, projednala Komise pro etiku ve výzkumu Fakulty sociálních věd Univerzity Karlovy žádost *„Řešení kybernetických hrozeb pro vesmírný program EU: regionální a mezinárodní spolupráce“,* podanou paní Michaelou Dvořákovou (Submission #69). K uvedené žádosti, jejíž podoba je na vyžádání k dispozici na Fakultě sociálních věd, nemá Komise pro etiku ve výzkumu žádné výhrady a vyslovuje souhlas se záměry předkladatele.

Komise pro etiku ve výzkumu schvaluje žádost bez výhrad.

S pozdravem,

Emil Aslan

Emil Aslan
Člen Komise pro etiku ve výzkumu
Fakulta sociálních věd Univerzity Karlovy

Univerzita Karlova, Fakulta sociálních věd / Smetanovo nábřeží 6, 110 01 Praha 1
info@fsv.cuni.cz, tel: 222 112 111

www.fsv.cuni.cz

Appendix no. 2: Informed Consent Form (EN version)

Informed consent to be interviewed for the research purposes of the Master's thesis Tackling Cybersecurity Threats to the EU Space Programme: Regional and International Cooperation.

By signing, I consent to the following points:

I was informed about the purpose of the interview, which is to collect data for the research needs of Michaela Dvořáková's diploma thesis under the title of Tackling Cybersecurity Threats to the EU Space Programme: Regional and International Cooperation.

I have received sufficient information about the research interview process. I understand that a transcript of the research interview will be sent to me to check the correctness and completeness of the answers. I am aware of my right to refuse to answer any question, to modify the answers retroactively, or to refuse to participate in the research within three days of the interview.

I consent to the recording of the research interview and its subsequent processing. The audio recording of the interview will not be provided to third parties and will be deleted after being transcribed. The transcription of the research interview will be freely accessible online as a part of the Master's thesis.

I am familiarised with how the research interview will be handled and how anonymity will be ensured after the research interview, which will make it impossible to identify my person. Neither my name, nor other personal information by which I could be identified, will be mentioned in the thesis, only the name of the institution I have worked at at the time of the research.

I give my permission to the researcher to use the research interview for the purposes of her thesis and to quote parts of the research interview throughout it. I understand that the audio recording of the research interview will be deleted after being transcribed.

Date:

Participant's signature:

Appendix no. 3: Informed Consent Form (CZ version)

Informovaný souhlas s poskytnutím rozhovoru pro výzkumné účely magisterské diplomové práce *Řešení kybernetických hrozeb pro vesmírný program EU: regionální a mezinárodní spolupráce*.

Podpisem vyjadřuji souhlas s následujícími body:

Byl/a jsem informována o účelu rozhovoru, kterým je sběr dat pro potřeby výzkumu diplomové práce Michaely Dvořákové s názvem *Řešení kybernetických hrozeb pro vesmírný program EU: regionální a mezinárodní spolupráce*.

Bylo mi sděleno, jaký bude mít rozhovor průběh. Bylo mi sděleno, že mi bude transkript odpovědí zaslán za účelem kontroly správnosti a úplnosti odpovědí. Jsem seznámen/a s právem odmítnout odpověď na jakoukoli otázku, odpovědi zpětně upravit, nebo odmítnout účast na výzkumu do tří dnů od poskytnutí rozhovoru.

Souhlasím s nahráváním výzkumného rozhovoru a s jeho následným zpracováním. Zvukový záznam rozhovoru nebude poskytnut třetím stranám a po přepsání bude vymazán. Transkripce výzkumného rozhovoru bude volně přístupná online jako součást diplomové práce.

Byl/a jsem seznámen/a s tím, jak bude s rozhovory nakládáno a jakým způsobem bude zajištěna anonymita i po skončení rozhovorů, která znemožní identifikaci mé osoby. Nikde nebude uvedeno mé jméno či jiné osobní údaje, díky kterým bych mohl/a být identifikován/a. V diplomové práci bude uveden pouze název instituce, pro kterou jsem pracoval/a v době výzkumu.

Dávám své svolení k tomu, aby výzkumnice použila výzkumný rozhovor pro potřeby své diplomové práce a některé části rozhovoru v ní bude citovat. Rozumím tomu, že zvuková nahrávka rozhovoru bude po přepsání vymazána.

Datum:

Podpis respondenta:

Appendix no. 4: Research Interview Questions

Tackling Cybersecurity Threats to the EU Space Programme: Regional and International Cooperation

1. Globally, most sectors have been recording an increased number of attempted or successful cyber attacks on their infrastructure. Has the EU space programme been perceiving the growth in cyber attacks in the past decade?

2. How are cyber attacks on space systems different from other kinds of cyber attacks in terms of intensity and severity? Which types of cyber attacks are the most common?

3. Does the EU space programme have a more preventive or reactive cyber security policy?

4. How has the EU space programme worked as a whole to prevent cyber attacks and/or become more resilient towards cyber threats?

5. How do the technical and political approaches of the EU space programme to countering cyber threats differ?

6. To what extent does cooperation exist in terms of regional and international intelligence sharing on cyber security threats and vulnerabilities throughout space programmes and institutions?

   - Has cooperation between the EU member states on emerging and actual cyber threats helped make the EU space programme more secure from cyber threats?
   - Has international cooperation on emerging and actual cyber threats to space programmes helped make the EU space programme more secure from cyber threats?

7. Does public-private cooperation exist in the space sector in terms of intelligence sharing on cyber security threats and vulnerabilities?

   - Has public-private cooperation on emerging and actual cyber threats to space programmes helped make the EU space programme more secure from cyber threats?

Appendix no. 5: Research Interview Transcript - ESPI participant

Interview 1: European Space Policy Institute Participant

Q1: Globally, most sectors have been recording an increased number of attempted or successful cyber attacks on their infrastructure. Has the EU space programme been perceiving the growth in cyber attacks in the past decade?

If you have a look at EU communication, whether it's digital communication, digital policies or security policies of the EU, where space cyber security or cyber threats on space systems are acknowledged, it's quite recent. However, this is not just the case of the EU, it's everywhere. It's only very recently that public policies have acknowledged cyber threats on space systems, so for a long time cyber threats were overlooked. You'll probably see only a few reports on the topic. When you look at the existing literature, it was only in political science that around 2012/2013, there were publications, academic articles on space cybersecurity, explaining that space cyber security was not really understood well in international relations debates, that it was too complex, and then too simplified, because it was addressed by political scientists, or people that do not have the technical background, so it was a bit misunderstood.

Then through 2013/2014, space cybersecurity was acknowledged as an emerging threat on space systems. There was this big report from Chatham House in 2016 on Space Cybersecurity: The Final Frontier, that stated cyber threats on space systems are really overlooked in space policies, or public policies in general, and this needs to change because we see increasing numbers of cyber threats on space systems. So, from there on, I think it was a breaking point after the Chatham House report came out. It became clear that a bigger understanding from the industry, from policymakers on these threats was needed. It was slow to appear in policies, but - I know that the authors of the Chatham house report consulted British space stakeholders and tried to explain the situation, tried to understand better cyber threats on satellites and how to raise awareness among the political communities. Apparently, this was a big thing that had not really been done before in the UK.

After that report a lot of other reports and publications took the findings of that Chatham House report and again, mentioned cyber threats on space systems are overlooked in public policies and people started to look to the US or other countries and slowly, until 2020, were starting to see that cyber threats were acknowledged in cyber policies, satellites were increasingly mentioned, etc.. So this is something that took a lot of time, but now it is more recognised, and if you look at EU policies - so in the digital policies, for instance if you look at the EU they acknowledge some cyber threats on space systems, mostly the security policies do that, the Cybersecurity Strategy for the Digital Decade or the Strategic Compass have a lot of references to space cybersecurity. They take examples and recognise that space systems are increasingly vulnerable. The EU policy on cyber defence also mentions space and cyberspace and it also took examples of real-life events; the KA-SAT attack at the beginning of the invasion of Ukraine, they acknowledged that, so I think this event was really a breaking point as well. Here, policymakers understood the ripple effects that this kind of attack could have on critical infrastructures, that connections between networks could really have an impact in other countries. That an attack on a system in Ukraine could then have ripple effects in the UK, Italy, France, Poland… This was acknowledged in the policy, so we can say that whenever an event occurs now, in terms of space cybersecurity, policymakers now take stake in it and acknowledge it in their policy papers.

If you look also at the NIS 2 directive, now, in Europe, space is considered a critical infrastructure, which was not the case until now, so this is also a major change. It increases the level of cybersecurity that space operators have to implement - there are stricter cyber obligations for operators. Of course it's just a directive, so member states have to implement it into their national law, so there's a bit of flexibility in the way it is going to be implemented, but at least it sets a framework and some kind of basic level of cybersecurity that should be implemented for space systems. I think that there is now a true realisation from EU policymakers that satellites are the single point of failure in critical infrastructures - so if you target a satellite and the satellite is enabling critical infrastructure like oil rigs, pipelines, smart grids, anything that uses a SCADA system, then it can disrupt the functioning of society and the economy, so I think now they understand this. But a few years ago there was not much understanding of this.

EUSPA manages a lot of the cybersecurity of the EU space programme, and at the beginning of Galileo, the cybersecurity obligations were really low, so they had to build everything from the bottom. I released a report a few months ago, we did an online conference on it, and Bruno Vermeire, who was the head of the Security Accreditation Board at EUSPA was invited, and he explained his experience on how cybersecurity evolved within EUSPA. I highly recommend it - it is on the youtube channel of ESPI and it will also give you an idea about the EUSPA approach. It was very interesting, because he was talking almost from a personal perspective - how things happened and how things evolved in terms of cybersecurity within GSA and EUSPA.

Q2: How are cyber attacks on space systems different from other kinds of cyber attacks in terms of intensity and severity? Which types of cyber attacks are the most common?

You mean all the kinds of cyber attacks on normal computers on Earth? I do not think they are that different in terms of intensity and severity. What is different is the orbital environment. So, I think there is not necessarily a big difference between a cyber attack on a normal computer and, for example, a cyber attack on a ground station, or on the control segment. I think it is more or less the same, what is different is cyber attacks on the satellite itself - on the space segment - when it is in orbit, because then you have the constraints of the orbital environment, which is naturally hostile and very different. Then the intensity and severity can change, but I would say the difference is very little. Especially now, when satellites are increasingly digitalised, they have an increasing number of software components, some of them are powered with IP protocols, so they are technically part of the internet, so today I think there are less and less differences. So you see a bit of a space and cyberspace merge in a way - maybe it is a bit of a strong word to say merge, but they are increasingly interrelated, so there are less and less differences.

Then the types of attack that are the most common - it is hard to say because we see a lot, and also because it's cyber, there is a lot of information that is not public. We only know so much about the attacks that are revealed and probably, most of them are not public, so it is hard to say truly which types of cyber attacks are the most common. I would say that the most common right now are attacks on the supply chain. So today - you can use the source of the EU media report on this, on supply chain cybersecurity - it is that companies understand the issue of cyber security a bit more, so they are protecting their systems, or their business, or whatever product they sell. But then the supply chain becomes a weak link, either because they forget about it, or because it is so difficult, because supply chains are so globalised, there are so many companies and subcontractors, in different countries, and different jurisdictions, different rules, different obligations, it is very difficult to secure them. Especially if you are not a huge company, or if you are a start up it is very difficult. Even if you are a start up you have an internationalised supply chain, because of the small components, the micro-processors, the semiconductors, they all come from around the world, so you have no choice but to have an internationalised supply chain. So, I think that it is a weak point now, and we have seen that in the past year. A lot of the attacks exploited supply chains, not only physical components, but also software components. So - a space company would sign a contract with a subcontractor, for example an overhead cost - software. I mean things that the company is using, not in the satellite system, but for its own business, so for example databases, things that the administrative staff is using. Or if there are no blocked connections, if there are no containers, separations in networks, then attackers can enter through that way. I think that is a big weakness.

The other biggest weakness is the user segment, or user terminals, so modems that people have at home, or that end users are using. This is usually very badly protected. It has been 10-20 years that cyber security companies are telling space operators to better secure user terminals, that they are full of vulnerabilities, unpatched vulnerabilities, zero-day vulnerabilities… And operators, because the modems are low-cost, easily replaceable, they do not realise how it can affect the entire space system, the entire infrastructure. So they do not really care so much about it. I think the KA-SAT attack, which affected the user segment and internet modems, created a wake-up call, and then operators realised - okay - so we have to integrate cyber security in that, and it is important. We have seen hardware cyber vulnerabilities on Starlink modems and so on, so now there is more awareness from satellite operators on this part too.

[on weak points - supply chain and user terminals] They are not really types of attack, but the most vulnerable segments. Otherwise for types of attack - this is really hard to say, I would say DDOS, but it is hard to say which are the ones that are the most common.

Q3: Does the EU space programme have a more preventive or reactive cyber security policy?

Interesting question, it is really hard to say because a lot of the acknowledgements of cyber threats on space systems are just that - acknowledgements. They are not necessarily policy measures. So they say - yes, this is a risk, it's increasing, we should protect our systems, but then there are no specific ways in which they want to do it. For the EU space programme, when it comes to the cybersecurity of Galileo for instance, then I would say more preventive, because there is increased encryption etc., so then I would say preventive, but in terms of EU cybersecurity policies, I would say more reactive.

If you look at the EU cyber diplomatic toolbox or these kinds of things, it's more reactive. It is about putting sanctions on cybercriminals and such, also anything that is related to cyber crime. I would say that policy-wise, it's more reactive, but for the EU space programme I think that in the past few years they really tried to be more preventive and increase the security overall. When it comes to reaction for the cybersecurity of the space programme, if you mean it as "can they hack back?", then I do not really know if that is something that they are doing. I would say that attribution, retaliation and so on is the job of the government, and it should remain the sole domain of the government, otherwise it would be becoming a little bit of the cyber "far west". Although you can find in the literature authors that advocate for companies or people to be able to do that. So you can find both arguments in the literature but I would say that it should be the member states that do it, if it affects their systems. For the EU space programme, I do not know what their policy is. I guess you would have to do an interview with them.

Q4: How has the EU space programme worked as a whole to prevent cyber attacks and/or become more resilient towards cyber threats?

They increased a lot of the encryption parts, they increased the security in general, so I think that in the regulation that established the EU space programme and EUSPA, you have a lot of provisions that mention cybersecurity and security in general. You can also have a look at the mandate and the work that the security accreditation board is doing. In general there is a lot of effort that was put in place to increase the general security of the EU space programme, not just for cyber threats but also insider threats. Most people working at EUSPA have a security clearance that had to be given by their member states. They really try to increase the overall security of the space programme.

Q5: How do the technical and political approaches of the EU space programme to countering cyber threats differ?

Q6: To what extent does cooperation exist in terms of regional and international intelligence sharing on cyber security threats and vulnerabilities throughout space programmes and institutions?

- *Has cooperation between the EU member states on emerging and actual cyber threats helped make the EU space programme more secure from cyber threats?*
- *Has international cooperation on emerging and actual cyber threats to space programmes helped make the EU space programme more secure from cyber threats?*

You have cooperation agreements for cybersecurity between states, but it is very rare that it covers space cybersecurity. So in general it is not something that is really addressed, however, you have cooperation in other ways. Through organisations like Space ISAC - if you have not encountered this organisation, it is a US based organisation for intelligence sharing and risk sharing on cyber threats on space systems. It includes US intelligence agencies and federal agencies, US space companies and some non-US space companies. There are also public space companies outside the US that joined, they are sharing risks, or whenever they encounter vulnerabilities, they share the patches between themselves. They are like "we noticed these threats, these kinds of patterns, these attacks have been happening recently, it could maybe also affect the space sector, so we are informing you about these". So it really is about sharing risks, threats, and vulnerabilities. It is a good way to share intelligence on cybersecurity threats on space systems.

Other Space ISAC are trying to be established elsewhere, it is something that countries increasingly find relevant, also in the EU, some member states are increasingly integrating space into their CERT/CSIRT. For instance in the French national cybersecurity agencies, now there is someone specialised in space - this was not the case ten years ago. So this is changing, and you can also see increasing research in space agencies, or initiatives in space agencies, to either do technology development on space cybersecurity, or to better study space cybersecurity because for a long time, the space community and the cyber community did not really interact with each other. This did not fully enable research to truly understand cyber threats on space systems and especially on the orbital segment, to understand the constraints of the orbital environment. How the hostility of the orbital environment, and how far the satellites are from the Earth can have an impact on encryption, on cybersecurity measures, because usually, traditional cybersecurity measures are implemented. That means that operators usually implement traditional cybersecurity measures for normal computers on Earth, and sometimes they are not really adapted. Even communications from the FBI, CISA, the NSA and so on, they sometimes recommend solutions, so they would be like - "oh, we recommend operators to implement independent encryptions, and the operators are like - ok, but this is not really effective on the space segment" because the encryption does not always work because of how far the satellite is and because of the nature of the orbital environment. So these are the kinds of things where more research needs to be done, and we are seeing, in the past three years I would say, some more research and more interactions between the space and the cyber community.

Nothing comparable to space ISAC exists within the EU, but European companies can join Space ISAC. There are not many European ones, but it is possible, it is inclusive of other than US ones.

I do not think that international and EU cooperation is really comparable. For international cooperation it is very different. For the EU, there is the EU space programme, where there are rules for member states, and the cybersecurity of the EU space programme is distributed in many member states, so you have one organisation in Italy with its own tasks, one in France with its own tasks, in Spain too - it is very widespread, so you have to have cooperation. But this is not really comparable to what space ISAC is doing. You need to have cooperation to ensure that there is consistency in Europe, across all the components of the EU space programme, on the trusted entities that are implementing -- because EUSPA is overseeing most of it, they don't really do the cybersecurity, it is delegated to trusted entities in different member states most of the time. There is cooperation in that sense, but I would not compare it to international cooperation. It is rather different.

Q7: Does public-private cooperation exist in the space sector in terms of intelligence sharing on cyber security threats and vulnerabilities?

- *Has public-private cooperation on emerging and actual cyber threats to space programmes helped make the EU space programme more secure from cyber threats?*

Space ISAC is a good example of this, because it really puts public and private stakeholders at the same table. In Germany, you can see the government cooperating with space companies, with actors like AirBus, to study space cybersecurity, to establish recommendations on space cybersecurity solutions, to identify the greatest threats. They issued a report recently on this issue, where they mostly assessed threats on the ground segment, with some risks and solutions and particularities of space systems. So you can see this kind of public private cooperation. There is an increasing number of space cybersecurity companies, which was not the case a few years ago, and of course there is cooperation with public actors to have a better understanding of their needs - companies like CYSEC (based in Switzerland) for instance are doing a lot in Europe. CYSEC has some space cybersecurity products and signed many cooperation agreements with public entities.

Then it really varies from one member state to the other, but in some member states there is true cooperation and constant communication between public actors and space companies regarding security threats in general. Not just cyber, but also intellectual property theft, industrial espionage, or other - so it varies a lot from one country to another, but this is something that member states are increasingly doing.

Overall, the space sector is a very small sector, so if there is an increased awareness on cybersecurity threats on the space infrastructure in this sector as a whole, it has a benefit for the entire sector. It sets some standards, you have initiatives, forced standardisation, best practices, you have more interactions on what are the current threats, what are the solutions. For the EU space programme per se, it is the regulation that is establishing the EU space programme that is setting the rules, as well as other EU legislation. I would not say it is that related, but the EU is trying to do more public/private cooperation in its flagship programmes - the IRIS2 constellation will have significant public/private cooperation. It creates new types of cybersecurity risks, because you have to bet, and the objective of the constellation is to be secure enough for government communication and secure communication, so it has to be secure enough for this, but it also has to be flexible enough for commercial applications. Especially for 5G, IoT, smart city, these kinds of things, where you need extremely good latency, and security is usually making the data processing and data connections much slower. This is a challenge. The right cybersecurity framework will have to be set up for the constellation as a whole, so the idea at the moment is to merge it with the EuroQCI, so you have quantum encryption. This is one solution that they want to implement, but it cannot be limited, the cybersecurity of the flagship programme cannot just be limited to that.

So, how do you protect against cyber threats during the development of the programme, when satellites are being manufactured by contractors? How do you secure that? Do you put obligations to have Faraday cages, or that space companies have to build these kinds of satellites in separate facilities from the commercial satellites that they build? These are the kinds of logistical obligations that you can implement that can increase the cybersecurity of an entire system - from the manufacturing stage, the supply chain, to the launch. It has to encompass each step of the development of the project to have real cybersecurity. The public/private partnerships create challenges, so it remains to be seen how this will be tackled.

Appendix no. 6: Research Interview Transcript - EUSPA participant

Interview 2: EU Agency for the Space Programme Participant

Q1. Globally, most sectors have been recording an increased number of attempted or successful cyber-attacks on their infrastructure. Has the EU space Programme been perceiving the growth in cyber-attacks in the past decade?

Yes, the EU Space Programme has been perceiving the growth in cyber-attacks in the past decade. Like other sectors, the space domain is not immune to cyber threats, with an increasing number of attempted attacks in general.

Q2. How are cyber-attacks on space systems different from other kinds of cyber-attacks in terms of intensity and severity? Which types of cyber-attacks are the most common?

Cyber-attacks on space systems differ from other kinds of cyber-attacks in terms of potential impact on critical infrastructure, the vastness of the affected area, and the potential for cascading effects. Cyberattacks on space systems can target data, transmission, and control processes in satellites, ground stations, or end-user equipment. Some of these attacks can be executed with relatively low resources and can be contracted out, making them accessible to various state or non-state actors. Cyber-attacks on space systems can lead to loss of data or services, systemic disruptions, or even permanent satellite damage. Attribution of cyberattacks remains challenging due to the various methods attackers use to conceal their identities.

Q3. Does the EU space programme have a more preventive or reactive cyber security policy?

Both prevention and reaction are important. Identifying potential vulnerabilities and addressing them proactively is as important as responding to incidents as they occur.

Q4. How has the EU space programme worked as a whole to prevent cyber attacks and/or become more resilient towards cyber threats?

The EU space programme has worked as a whole to prevent cyber attacks and become more resilient towards cyber threats by implementing comprehensive security frameworks, raising awareness of cyber risks and fostering inter-institutional cooperation (ENISA, CERT-EU).

Q5. How has the EU space programme been working on countering the increasing number of cyber threats? How do the technical and political approaches to countering cyber threats differ?

The EU space programme has been working on countering the increasing number of cyber threats through technical measures, such as security requirements, security by design, and improving the security of systems and infrastructure.

Political approaches, such as promoting international cooperation and the establishment of norms of responsible behavior in cyberspace, are prerogative of the European Commission. While political approaches aim to create an environment where cyber threats are minimized and cooperation is sought with different entities and institutions, the technical ones focus on minimizing the identified vulnerability and keeping pace with the technological development of the systems.

Q6. To what extent does cooperation exist in terms of regional and international intelligence sharing on cyber security threats and vulnerabilities throughout space programmes and institutions?

- *Has cooperation between the EU member states on emerging and actual cyber threats helped make the EU space programme more secure from cyber threats?*

Cooperation between EU member states on emerging and actual cyber threats has indeed helped make the EU space programme more secure from cyber threats. Sharing intelligence and best practices enables the EU to identify, assess, and address vulnerabilities more effectively.

- *Has international cooperation on emerging and actual cyber threats to space programmes helped make the EU space programme more secure from cyber threats?*

International cooperation on emerging and actual cyber threats to space programmes has also helped make the EU space programme more secure. Collaboration with international partners contributes to the exchange of information, the development of shared standards, and the fostering of a global culture of cyber security.

Q7. Does public-private cooperation exist in the space sector in terms of intelligence sharing on cyber security threats and vulnerabilities?
a. Has public-private cooperation on emerging and actual cyber threats to space programmes helped make the EU space programme more secure from cyber threats?

Public-private cooperation in the space sector in terms of intelligence sharing on cyber security threats and vulnerabilities is an emergent field of activity. Collaboration between the public and private sectors is deemed essential, as many space technologies and services are provided by private companies.

Appendix no. 7: Research Interview Transcript – CGI IT Czech Republic participant

Interview 3: CGI IT Czech Republic Participant

Q1: Globally, most sectors have been recording an increased number of attempted or successful cyber attacks on their infrastructure. Has the EU space programme been perceiving the growth in cyber attacks in the past decade?

I think that this is the typical question where I'm not sure whether I am the right one - the relevant one - to answer this question, because I am not the owner of some particular data pack of cyber attacks. I think that the EU, through EUSPA, has their own programmes for the detection of cyber attacks on European space programmes. But based on the information I work with within the market I think the answer is yes. Definitely, even in the European space the number of cyber attacks is increasing.

Q2: How are cyber attacks on space systems different from other kinds of cyber attacks in terms of intensity and severity? Which types of cyber attacks are the most common?

Again - I only work with the data I have access to. I think that it really depends on what the goal of the cyber attacks is, and what the attackers aim to achieve. For example, from my experiences, I am aware of attacks which are used on the tolling systems used in GNSS technologies and these attacks are typical ones - it's not done to destroy the system or to somehow attack the system, but to avoid the duty of paying the toll. And of course there are some kinds of attacks based for example on the spoofing principle, to give the receiver wrong information about the governed position, but I think that this is still not very common, it is not daily-life attacks with some particular aim it is still more of a theory which has been proven several times, but this definitely is not the majority of the attacks aiming at something particular, in my experience.

Q3: Does the EU space programme have a more preventive or reactive cyber security policy?

Again- this question should be dedicated to someone representing the EU space programme from EUSPA, ESA, or even the European Commission. In my opinion, the answer is again yes, not just the policy, but even the activities that definitely lead to a more proactive protection in regard to cyber attacks.

- *Would you say that it is transforming from more reactive to more preventive?*

Both - the prevention is key, but of course to be able to react with mitigating the risk of damages is also very very important.

Q4: How has the EU space programme worked as a whole to prevent cyber attacks and/or become more resilient towards cyber threats?

It is hard to say. Of course it is somehow harmonised within the whole European space programme, but I think that the type of cyber attacks differ from various space programmes. I think that right now, for example the Galileo programme and the positioning and timing services are more sensitive to cyber attacks than for example the Copernicus programme and the earth observation data. I think that some mutual communication approaches exist but still, for each programme I think that the sensitivity of protection and the approach itself is quite different.

Q5: How do the technical and political approaches of the EU space programme to countering cyber threats differ?

I think this goes hand by hand. One could not exist without the other.

Q6: To what extent does cooperation exist in terms of regional and international intelligence sharing on cyber security threats and vulnerabilities throughout space programmes and institutions?

- *Has cooperation between the EU member states on emerging and actual cyber threats helped make the EU space programme more secure from cyber threats?*
- *Has international cooperation on emerging and actual cyber threats to space programmes helped make the EU space programme more secure from cyber threats?*

Definitely. This is again - all the member states try to be somehow harmonised. For example - I am not sure how much you are aware about the Public Regulated Service of the Galileo system - so the general idea is that each member state has their own PRS CPA (Competent PRS Authority), which is somehow the centre of the PRS service within each member state. These entities have their own autonomy to decide whether the PRS would be used in the member state - which user groups will have access to the PRS, how many final users there will be within the country, etc. But also - all the CPAs should be connected to some European centre and I know for example that the representatives of each CPA meet on a regular basis, they regularly discuss for example with EUSPA, they contribute to the development of the service, so in these terms there is definitely some kind of harmonisation within the entire EU. Still, there is a big autonomy of each member state, each particular country.

Q7: Does public-private cooperation exist in the space sector in terms of intelligence sharing on cyber security threats and vulnerabilities?

- *Has public-private cooperation on emerging and actual cyber threats to space programmes helped make the EU space programme more secure from cyber threats?*

Definitely. There is a deep and long-term collaboration between the public and the private sector. Even our company is a great example of this. Our company is the biggest Czech supplier with regard to EUSPA, this means that we are providing space security oriented services to EUSPA. So there definitely is a collaboration - and it is not just our company, but also our competitors or even partners. So definitely the organisation EUSPA is collaborating with the private sector and I think that a part of the provision of this service is even the knowledge gained in other markets, other segments, and sharing the best practices which could be applied towards the EU space programme. On top of this, private companies share intelligence on space cybersecurity amongst themselves. Even the core of all the space programmes is based on the knowledge and delivery of the private sector companies.

Appendix no. 8: Research Interview Transcript – CYSEC participant

Interview 4: CYSEC Participant

Q1: Globally, most sectors have been recording an increased number of attempted or successful cyber attacks on their infrastructure. Has the EU space programme been perceiving the growth in cyber attacks in the past decade?

This is not within my field of knowledge, you will have to ask someone from EUSPA.

Q2: How are cyber attacks on space systems different from other kinds of cyber attacks in terms of intensity and severity? Which types of cyber attacks are the most common?

Are they different? Yes and no. To operate the satellite you need a ground segment, and this is very much standard IT - so you have a cloud service, you have servers, you have connectivity on the ground, fiber optics, you have software running on these servers or on these cloud services, mission control, computers, laptops. All of this is the same as if you were doing financial services or any other type of service. The only unique thing is that you are operating an object that is orbiting at 500 or 36 000 km above your head, which seems to be far, but this object is still connected, right? So it is still you who needs to operate it, or the downlink, and have access to the data and the information it is collecting, but so can the potential attacker. So that is the question of the attack surface, which is bigger for space assets because you have all this stuff on Earth, and also the tip of the iceberg, which is the satellite itself.

So are the attacks different - again, yes and no. No, because when the satellite is in orbit, the only way to attack it or to do some damage to the satellite is through the ground segment, which is again through all the standard IT stuff - so Linux OS and all that stuff which is very similar to financial services and similar. But the other way you can also harm a satellite is to attack it when it is still on ground. This is the part that most people underestimate or miss - vulnerabilities occur as soon as an engineer starts designing an architecture or a space system. So as soon as you have a team working on a mission, on a satellite, if this information leaks, then it can be potentially compromised. So all the development phases, from day one in the design phase all the way to the launch, when the satellite is actually sitting on the launchpad and waiting to go, this is all very sensitive in potential attack scenarios. We have seen this during testing, during assembly, during development… you name it. All these phases on ground, they are all potential attack scenarios.

Q3: Does the EU space programme have a more preventive or reactive cyber security policy?

This is hard for me to say, because I do not work for the EU space programme. This is insider information that is hard to come by.

Q4: How has the EU space programme worked as a whole to prevent cyber attacks and/or become more resilient towards cyber threats?

Unless you have been working in the EU space programme as an insider, it is hard to know the answer to this question from the outside. There are no public press releases saying "Galileo has been attacked 10 times today and we almost died and recovered safety at the last second". So unless you have really been working inside the team, nothing of this sort goes out publicly.

Q5: How do the technical and political approaches of the EU space programme to countering cyber threats differ?

All I can say from an outsider perspective is that if you take for example Galileo - very sensitive service obviously, for European sovereignty, so I always take Galileo as the example of one satellite constellation being very well secured, because the Commission has been piling really billions of taxpayers money into securing Galileo. Because it was so sensitive, right? So we could not really afford to have it taken down by the Russians or the Chinese. We really put so much money, so much effort into Galileo security that it was almost too much. That is my personal perspective, my personal opinion on the matter. I have seen engineers working on risk analysis reports that nobody reads at really expensive hourly rates, that it was too much taxpayers money to justify - again, this is just my personal opinion.

This is challenged by the way that the Commission wants to design IRIS2, which I think is a good example of another use case - another example of an EU constellation we are trying to develop which has a much lower budget, and as much stringent security requirements because they want to accommodate commercial service, dual-use, governmental services even military almost. So it is a really difficult challenge to have all these requirements in one single constellation. Here, there is a more pragmatic approach in allowing start-ups to be on board and to develop innovative services and technologies with less heritage in the space industry. I think that is a good example of how we started first with Galileo which is a success, but very expensive for the taxpayers money, to IRIS2 which is going to try to be as good as Galileo, maybe even more agile, more versatile, more useful in a way for EU citizens and with a better use of the allocated budget.

Q6: To what extent does cooperation exist in terms of regional and international intelligence sharing on cyber security threats and vulnerabilities throughout space programmes and institutions?

- *Has cooperation between the EU member states on emerging and actual cyber threats helped make the EU space programme more secure from cyber threats?*
- *Has international cooperation on emerging and actual cyber threats to space programmes helped make the EU space programme more secure from cyber threats?*

If I answer this from my window of expertise, which is more industrial and business oriented - more 'New Space' if you wish. There is no information sharing whatsoever. Companies do not talk to each other - there is no public agent supervising all of this and that distributes all the gathered information from relevant players. That does not exist today. The only public effort I know of is the Space ISAC which was conceived in the US, trying to convince European players to come on board and to join the association. Whether it is a good idea to go with the Americans or to try our own ISAC as a European thing is something open for debate. However, everything needs to be created or adapted based on this existing space ISAC and currently, nothing is being implemented from a business perspective, so I am not talking about the agencies - I do not know if EUSPA is sharing their information - on this I have zero knowledge. What I know is that businesses in the space industry - private businesses - have very limited information sharing between each other and with the public entities.

Q7: Does public-private cooperation exist in the space sector in terms of intelligence sharing on cyber security threats and vulnerabilities?

- *Has public-private cooperation on emerging and actual cyber threats to space programmes helped make the EU space programme more secure from cyber threats?*

There is very limited public-private cooperation and intelligence sharing on space cybersecurity issues. That is the situation as it is today.

Appendix no. 9: Research Interview Transcript – Chatham House participant

Interview 5: Chatham House Participant

I will start by giving you the overall geopolitical context of cybersecurity in space, which is more of the Chatham House way, because the cyber domain is quite complex, and you need this context to fully understand what is going on.

So, in sophisticated cyber-attack organisations you also got the organised criminal gangs, which normally go for the commercial gain. And the problems you've got there is that Putin and the Kremlin has looked as though he's now recruiting or using them as additional attackers to help his government. It is a government APT type of thing, so that's the problem with mobility of cybersecurity threats.

So organised criminal gangs, normally go after money, but Putin pays them a few million to help him out, attacking western infrastructure and doing other sort of stuff, and much as you would recognise your individual hacker, who would then be recruited by an organised criminal gang for the special skill that he or she has got, in terms of ways to get into a system and it's a very mobile market and it's very difficult to pin people down, but of course now we've got the problem and I think the timing is correct. Now Ukraine is a concern and obviously, there's the military, but cyber is part of the battle spaces, now including space and the land, sea, and air.

What we've got is now we've got Xi, who has gone and had a chat with his good pal Putin. Xi is on a different trajectory. My analysis is that China is on an economic quest for hegemony. It's why they have Belt and Road, why they're signing off all these deals now. And of course, I had a visit to Saudi Arabia back at the end of last year and Saudi oil has now been quoted not only in dollars, but also in Chinese Yuan, which is interesting. And he's visiting, if you track where Xi has been visiting, DRC, where they got the cobalt, they got a huge rock lithium deposit as well and so on.

And what you've got, is the Western side, the American side, where there's an industrial military complex wanting to go around the world, imposing themselves militarily as a hegemony, but there's your kind of your – Korea, Vietnam, Afghanistan history, and China trying to win it by trade and this is very interesting, because you've got this dissimilarity of two power blocks right and we'll get to the point about cyber in a minute, the two power blocks going like this, but what you've got, is Xi has now got the crisis in Ukraine. My analysis is, he's using that to fix the attention of America and the allies like the United Kingdom and Europe and Germany and France and so on.

To fix the attention once he continues his campaign, all that Belt and Road, Made in China 2025 policy, which China has been developing ever since Deng Xiao Ping, post Mao. 2005 was their first thing: like OK, here we go, and we all know that China has got a massive capacity for cyber security, or rather insecurity. Their GCHQ equivalent for GCHQ, where GCHQ has 7000 or 8000 cyber attackers, and China has got 130,000 cyber attackers in the fourth People's Liberation Army, so in terms of cyber, you've now got a very uncertain world, different power plays going on and of course cyber, because of our dependence on ICT systems everywhere, it is a very vulnerable attack surface. There's an awful lot of attacks going on in Ukraine, there are other attacks going on aimed at the United Kingdom. I certainly know that many of which are being repulsed by very good work by GCHQ and indeed by our industrial sector as well, because we've been on a cyber security path for about a decade, since the formation of the National Cybersecurity Centre, it's much more public facing and educational.

So, my background in cyber is mid to late 1990s but then this was called information warfare. I was on a cross departmental cabinet official committee in Whitehall when this type of thing first kind of kicked off. So now for the last 23 or 25 years I’ve been around some of that stuff. Anyway, so - Chatham House Fellow, and you'll see that the paper I've done in cybersecurity and space, which I did with Patricia Lewis, and I think that had a nice catalytic effect.

I've also done contracts for the UK space agency in raising awareness inside the UK space sector about cyber security. I think again one of the big vulnerabilities, here is it's as you are investing in your as a SMB let's say and you've got a nice new space related product that you've invented and it's a TRL 3, when you're trying to fund it to get it to TRL 4, so what is the balance of your investment in cyber security, where what you're trying to do is to develop the product, but also put a bit of money on the table, so you can actually eat and heat your house, which is increasingly challenging these days.

Cybersecurity tends to get forgotten and I think one of the key areas here and one of the weaknesses in ENISA and then NIS is that we really need a status today about what is actually whizzing, in a geostationary sense, around the world right now, go and do a back order saying which ones are the vulnerable satellites, the up and down links and indeed the ground stations including the dishes, which ones in the light of this new this new world that we're confronting, which ones have we overlooked the cybersecurity 10 years ago, that we haven't put the right investment in and therefore we've made ourselves open, such as through Chinese chipsets, how many people, how many organisations, when they were their sort of technical offering at TRL 2, when for your own money you probably mortgaged your own house, and you see a chipset from China at $10, but your alternative is one from United States $50?

Well, I prefer probably $40 so I can put shoes on my children. Do you see what I mean? So, there's an awful lot of stuff whizzing around now, so does it need to have a strategy to look back a bit and say - OK the stuff that we've actually got whizzing around - how vulnerable is it to a cybersecurity or a cyber-attack intervention? And what can we actually do about it? Do we put a probability score against it and say, it's reliability is maybe C in terms of is this something we can depend on and therefore use it for the management for critical national infrastructure, or are we going to find that it is going to fail suddenly, because it's so vulnerable, hackers have been in there and they're just going to do a 0-day exploit, press a button and all of a sudden it's going to fall over and then we aren't able to read our gas metres anymore or all those things.

The key thing here, which is also coming up, which I think is especially pertinent, is the fuel use, because we have a military crisis and it's always been known that in times of conflict, tension there will be a lot of offloads of military hardware, where the communications required expanded so much, that they'll be offloaded from the military systems, which obviously have high capacity for, generally the world order, you will then have a crisis. We think we need an awful lot more comms, we need a lot more EO and so on. It is a lot of your military, most probably the admin stuff, the logistic stuff, the welfare of the personnel, the soft logistic infrastructure, just to have people send monthly reports or just that mush, general mush, while the military side does the battle, but life must go on.

Do you have this offload into the commercial, so they just going higher bandwidth from Airbus or Northrop Grumman or wherever, but then what you got there is that, if you haven't nailed down those dependencies in the commercial life then your military systems and there will also be linkages between the two, so one, is there a pathway to get back into the military system through the current commercial systems that you have co-opted, which is an interesting attack path.

I'm sure they've tried, and I don't know how well they've done, the bad people. And also how, if you did lose some of that commercial traffic and then have to push it down into cables and stuff that goes under the oceans, which of course is another question, because we now know Russia's looking at undersea cables quite carefully. We learned from 1914, didn't we? So, the other problem we have got there, only in the last - oh no it was not funny - so you might have seen my Chatham House op-ed on cybersecurity. It's to do with China - and China's options in terms of how Xi can help Putin and one of the instruments that it the histories then goes back to 2010, when Japan arrested a Chinese trawler in the seven-dash line around the South China Sea.

So, in 2010 Japan arrested the trawler, a Chinese trawler, it was in the disputed area, Japan was very confident. They took it into harbour and China said, ‘OK unless you release that trawler, we are going to stop your supplies of silicon’, which they did and about a week later the trawler was released with all the ‘sorry about this misunderstanding’ and it was silicon for the Japanese semiconductor industry, and it was all sorts from China. So, China understands from that the political leverage that it's got in terms of critical minerals supply and of course our space and satellites and our ground stations and everything that consumes an awful lot of critical minerals of which right it now and we will get to the cyber aspects, China now controls 80% of global supply chains of critical minerals. In December 2020 it formalised what had been done in 2010 about the trawler, about the fishing boat, into law. So, if China feels upset with another economy, it can command and some of this they already did last year, it can tell, if the supply chains of these critical minerals, which it controls 80% of the overall stock, to stop providing critical minerals to A, B or C and last year they did it with Lockheed Martin, so they put that more law into place. That includes Chinese controlled enterprises worldwide so they might own a mill or a refining centre in DRC or something like that, and they put that law in place last year or against Lockheed Martin, that was building F35 for Taiwan, so we then said OK, where does this leave us in terms of size of security?

The next thing is that China sees commercial space assets. You have to prove the negative, you've got to prove that these space assets are not going to be used for military purposes. Now, from the military, they could ring you up and say, send me some useful bandwidth and I am trying to say, well you haven’t approved this, so it can constrain the supply of these critical minerals for commercial space and satellites. Combined with the understanding that it has about the cyber security infrastructure of global supply chains, critical minerals and cyber things make a really potent weapon in order to make European, British and I didn't think we're part of either anymore, but we're still part of ESA, which is nice. American commercial satellite and space systems are highly vulnerable to Chinese interference. And you combine that with what you then have left, which narrows the attack surface for their cyber folk to actually go on the attack to a much narrower supply chain than it actually had to concentrate on before.

So you got this horrible sort of circumstance and Xi announced two Fridays ago, after I published that Chatham house paper, saying we've got to watch out for Xi, and about a week later he actually followed my script, so I hope he wasn't reading my Chatham House paper, so that's a good idea, but he then says we don't want this Ukraine crisis, we're going to help our good friends, he's just using Russia as a tool. Russia should know this. Xi is fishy and that's all there is, he is in it for China. But he declared, here are some things we can do, and the foreign minister last Friday said, we're now going to have a look at intercepting, he says, Quin Gang, we're now going to look at supply chains and make our judgments on business services coming out of China which the West uses. You can think of that as narrowing the attack surface for China and all they do is fight the rest. Also, if there isn't also a 0-day exploit, they are already resident in the stuff that we've got airborne right now, because culturally, they play a long game. Getting a little bit of a software package, which is in the Tier 4 supply chain, a little chip set which was bought a few years ago on the open market, when we were friends with China. We had this new beginning under our Prime Minister David Cameron and George Osborne.

I'm just going to go through some of the points that you raised here, but I think strategic context might be useful in your paper, because the world's changing. It's changing really fast and one of the problems you've got in terms of ENISA and the EU, and I know that we're talking about the EU here, so I'll talk much more about this strategy.

I think the pace of change is what concerns me, because 18 months ago we're all fine and there was lots of grain everywhere and everyone was concentrating on Paris 2050 and of course then the world changed. And the world is changing too fast one converse, where we've got 27 nations and think about the EU - there is fair distribution of responsibilities and fair commercial opportunity within the big programs. What we've got there, I believe, Michaela, is a mismatch in the pace of events that China or Russia is able to generate in a month.

I made an equivalence this morning when I was researching - about Captain Phillips. It's based on a real-life incident of a captain of a cargo ship going around the Horn of Africa, where all the pirates are. I think they resolved it now. They were attacked by Somali pirates and his ship was actually taken over. So, what he had around his ship was this threat of pirates, in agile small boats, but lots of them, and they wanted to take over. And their kind of linear defence you have fire hoses to shoot water down onto the boat, barbed wire, and an armed guard. There was a refuge and the company of the ship, once the ship was taken over, they went down to this kind of strong room, near the engine.

And I think the European Space, and this is not individual to European Space, is we've got this relatively un-manoeuvrable big entity; it's got its defences, the firing hoses, the barbed wire, and things like that. It's got its refuges, where when everything goes to wrap, you go down into this strong room, where the bad guys can't get in, but what you have there, is you've always got the same sort of construct, that you have got your ICT systems - including space of course - and you've got your defences, which is great. These are your equivalent fire hoses to scare the enemy off and make it difficult to go through your firewall, and your antiviruses, and stuff like that, but once the enemy gets onto the ship, you're actually in the same kind of space.

In the end the United States Navy turned up after a few days and everything was resolved, but I think the concept is a bit like that. And I think the ENISA policy is trying to get everyone to be sensitised about cyber security from anyone who sweeps the shop floor all the way up to the chief executive of a satellite company, but one wonders, whether the commercial providers are yet fully sensitised to the risks about cyber-attacks. Now actually we're becoming more like cyber security means less profitability, less dividends to shareholders, less bonuses for the chief executive. I am worried that in the end you will get that in terms of your cybersecurity response like the United States Navy coming up, but one wonders about the integrity of the whole and where there's a lot of defence, but not enough defence in depth and security. This would not be uncommon in large scale collaborative enterprises like ENISA, but the key thing there is the pace of change.

Q: Do you think that this could possibly be solved, at least partially, by the NIS 2 directive?

Well, I've got the NIS down here - because what you have seen in space supply chains, it's heavily internationalised. So, does a specialised manufacturer in the states, who is producing something under a baseline of the NIS standards, which are pretty good, I mean they they've translated NIS into 16 languages or something, so it is established, so yeah - that's an interesting fact, they needed to have actually taken time to. And it's not Google Translate, they formally translate it to make sure there are no misinterpretation in A, B or C, they've got real translators to translate into any number of languages, I think now it's 16 languages and every time they issue a change to a particular standard or particular policy, they translate it again.

So, where does NIS stand with Europeans with ENISA? I'm not too sure, but one would generally hope that there is a close cooperation and I have recommended before to our UK cyber security industrial players, is that if there was just anything to do, because your little thing is going to end up in an international supply chain, just make sure you actually comply with the NIS 2 themes. Make sure also, which is a very weak point everywhere, make sure the boardrooms are sensitised for cybersecurity and the implications of company value, if they get it wrong as we can see lots of things like share price, property - TalkTalk, if you remember that.

It was first of its kind and it came out of British Telecom and somebody else who created this joint venture TalkTalk, these were fully integrated, so you could get your telephone, your Internet, your television, all that stuff, you get a talk-talk contract, and we'll sort it for you a little. Little bit like Sky. Anyway, their share price was launched around 50 pence, and everyone loved it. Then they had a hack, and they went from 50 pence to about four pounds per share. OK so the boss was this lady called Dido Harding, [redacted] and they had a hack, and they were up and about sort of 4 pounds a share from 50p over a 2-year period.

They had a hack and the attacker, who was a 19-year-old kid from the Northeast of England, got the hold of names, addresses, account numbers, bank details, basically all of the PI. It was a feast, because he then reposted it into the dark web and suddenly the little rumours started. And the key thing was, Dido Harding, who was a Baroness, or still is a Baroness, appears on a current space program, but she was unable to answer the question whether the data was encrypted. She said that about encryption 'I really haven't got a clue'. Check. Share prices fell off a cliff. And it wasn't encrypted and so you have all the PI, accounts, bank details, addresses, all of the things that you needed, a number of mobiles, one for my daughter, one for my son, one for my cousin.

So, it's the boardrooms, inside the European Space sector, are the boardrooms sensitised to the economic risks, if they don't pay proper attention? Triggered by Ukraine and this thing and I'm getting it even with our government agencies here, but [redacted] And this is what the stack, the industrial stack, has got to understand inside the European Space industrial complex is that this is everyone's problem now, because the world's really weird, if I can make that point.

There is this thing, because they're internationalised supply chains, which is the default mechanism you go for. Are you going to ask American companies or even Brazilian companies, they might be providing a really innovative 3rd tier piece of technology, what standards are they having to go through? Is it the end user ones or is it the NIS/NIST ones? One of the dissimilarities, have they investigated their supply chain all the way down to see if they've cyber vulnerabilities inside their supply chain as well? How do they prove it, and this is difficult stuff, so I'm worried whether ENISA is able to cope with the pace of change?

Space is one of the reasons the UK left the EU. The EU can be a little bit slow, and the enemy is not hindered by having bureaucratic processes. They'll just go and make mischief questionnaires about how much stuff has already been embedded in our supply chains. Actually, have a look at some of your vulnerabilities, 4th echelon, how do you want it, what is already airborne, how do you audit cybersecurity through technology TRL 2,3,4,5, what is the level of investment, is that portion sensible, are they concentrating on the right things, and how do you audit it. You might have heard about what's happening with our National Health Service. It's in complete disarray, wonderful people at the bottom end, I had experience, [redacted], they're brilliant people, intensive care, and accent emergency, but the bureaucracy. Oh, never mind, I should not go there.

Anyways, this is what happens if you discover a vulnerability in your system. This is your source of profit, this is your life passion, this is what you've invested in, and you discover a vulnerability from way back, when it was TRL 2. Are you actually going to declare? Do you see what I mean? But we left the door open, there it was, for about six months and any little zero day could have sneaked into our millions of lines of code. Are we OK with that?

We now have the Chinese foreign minister saying: we are now going to start getting naughty. They can't send troops to Ukraine. That would just be escalatory. They probably supplied intelligence already for Russia from Chinese satellites. It depends on whether they want the risk, meaning whether they would send any high-tech weapons to Ukraine, but then you have high tech weapons versus high tech weapons. Most of the Chinese ones are, well - the IP has been stolen from the United States. I wanted to study Huawei about how they, from virtually 0 R&D, turned into one of the biggest telecom providers in the world. Well, where did they get their idea from? Well, they just nicked it.

In terms of the questions there I hope I provided some sort of context about what needs to be done. If anything has to be done, it is to make sure that the ENISA bureaucracy - it mustn't be like this, you've gotta turn the pyramid. So, lots of action for the top-level board people, but then it's all about the speed of change, because if you can work faster than the enemy, which is probably unlikely, but if you work faster… this is how in military philosophy, it's how you generate combat power out of an inferior force. You just work faster. And pace is actually the key element here, so whatever is in place has to be configured. Does this promote pace or is it just going to turn into a bureaucratic nightmare and let the bad people have fun? And we have the backbone.

You see, in terms of the EU space program - I'm happy with cyber and the UK space program, provided I do fly this stuff for our space agency.

Q: How are cyber-attacks on space assets different from other kinds of cyber-attacks in terms of intensity and severity?

I think the key phrase there is, as more of our critical infrastructure is going into space, because the utility of space has increased, because it's cheaper launch and so on and so on as, as our national infrastructure migrates that way, it is more like, but certainly strategically, there will be a bigger threat surface because of the vulnerabilities, because there's more stuff going through space communications, there's more dependency on GNSS responsible for guidance of driving the vehicles, all that kind of stuff. As more of that happens the more utility you get out of the space, the more vulnerable it's going to be. Space will fix it! Yeah, but. Have you gone back to the 4th level of the supply chain? I think people are very glossy if that makes sense. "Space will fix it". Yes, it can, but… there we go.

Q: Does the EU space program have a more preventive or reactive cybersecurity policy?

Not an expert, but the key thing there is, developing policy needs to match the rate of change about how the threat manifests.

Q: Do you think you could possibly try to answer this from a UK perspective? I think that it would also be interesting to do a little comparison.

OK well I'll start off with three just to warm up because I can answer that from personal experience.

So, 18 months ago, maybe two years, I think it was earlier, I led a team from our satellite applications catapult UK space agency and one of our National Intelligence Authorities, to educate and it was a series of about 7 workshops, half day workshops, it was all done online. The first one is academia, so we spoke about mapping out outer space, the final frontier. We have the academics, the TRL 1, 2, 3s, the small to medium enterprises, government, and the big companies. And actually, one of the biggest problems is, the big people like Airbus and BAE Systems, they feel like: "We're fine." Why are you telling us this? We know this. Do you? [redacted] It's gone down in the UK space history of me being turfed out by Northrop Grumman, BAE Systems, Tardis, and all I'm saying is, the trend is changing, and they will say:

“Yeah - we're fine”. And now we find that there have been some really close calls. No, they're not fine. And the big ones are the ones that just have that default position of saying - yeah, we’ve got my IT department that looks after that. Is it on your company risk register? It's always a good start that your company recognises it.

Initially, you'll gross earnings per share, costing you millions of pounds to put in this ransomware, for the computer to start again and most often, it’s not the mid-range, it's the big ones that say ‘we've got an IT department, the one there - in the basement’. How much investment is your Chief Financial Officer going to make in cybersecurity compared to a PR budget, so you can go to trade shows and have flyers and a new online advertising campaign. What's the balance in terms of financial wellbeing? Compared to what happens, if you are under invested in the cybersecurity and somebody gets into your system, and he brings down the system.

I happened to be in the car with my cousin in Australia. She was then chairman of Telstra. Telstra have always said that yes, you pay more money, because we will provide you with 99.99999% availability. I was in the car with her. We just got over the Sydney bridge and there was an incoming telephone call. It was her chief IT guy. He says: “I think we've got a problem. The entire telephone system has been brought down by an upgrade of the system. A technician in Perth did something, and it introduced some kind of bug, and the whole thing collapsed.” And I've never seen my cousin look so calm, because you don't become chairman of Telstra for nothing, but you can see as she was driving along and she's just going through it all. There you have your gross earnings per share and Telstra had a real problem. Their big promise was availability, and this was a self-inflicted side effect, and the company value went down.

So, what is the balance that you have? You've gotta get it up in terms of your cyber security, there has to be a culture, where cyber is part of the company's risk. It's on the risk register, where you actually say, what is comparison between allowing our employees to have a bigger lunch allowance, so they can go buy nicer sandwiches and bag of crisps compared to my chief information officer coming to the CFO saying: “oh there's a new risk and we've got to do the following it's actually quite expensive.” and the CFO going: “right what are the needed actions? And the CIO goes: “This is what's going to happen”, or "Oh, that's going to be bad for us. That's going to run against our reputation, that's going to affect the share price, that means that the boss is going to be in trouble.” But she's going to have to report to shareholders. For the CEO, it is just another piece of paper, like say a request from the IT department. “2 million Euros! For what!? You can probably download this from the web”. This is a serious point. Who is going to sponsor this business protective structure?

Anyway, how does the UK space program work to prevent cyber-attacks and stay resilient towards cyber threats? There is much more investment now, it's been nice to see. When I first started working with the UK space agency and cyber, I'm thinking that there were three people, I'm thinking five years ago. It's now a team of about 20 or 25 people. And they are now also using this innovation agency called the Satellite Applications Capital to start in, which is an innovation agency for all UK space players to heighten awareness, sensitise people to concentrate on the value of the enterprise. So, what we've actually got is more realisation, more resources and I'm thinking, it's something like a five-fold increase over the last two or three years. It started from a low base, but then 25 people from 3 over two or three years is quite good.

And using the other toolkits that you've got our GCHQ, which has a public facing arm, or the National Side of Security Centre, who has now got a fully established space entity and the capital, and then the old kind of contractor like me. So, there's realisation, there is investment, we're on our way here in the UK.

Q: How can our space program work on countering the increasing number of cyber threats through the technical and political approaches?

Greater awareness is what you need, so I use the person from GCHQ as an example, because everyone wants to go listen to GCHQ, it's a crowd drawer it's like having a soloist, o these awareness symposiums, it is an issue of finding a vehicle to heighten awareness. And actually, as long as you get the messages right, to say this company: “don't have the boys and the girls from the basement at these events, because all the people who work in the ICT department, or who come from a programming agency won’t actually help. You need the bosses, you need the boardroom, that's where the key is, then you get the right investment. And of course, boardrooms don't understand super technical stuff, they just want to understand - who are the bad guys, who is my competition, how it's going to value, if I lose to the competition, what is the value of my business going to look like, give me some examples. And then you sensitise them, you get the right sort of investment and that's the program we did a couple of years ago and that really worked well. We're now getting to the next stage with that one and we're just going through the contract now, in order to enrich some of the messages.

Q: To what extent does cooperation exist in terms of regional or international intelligence sharing?

I think it's getting an awful lot better, certainly from the UK. We obviously have always shared intelligence with the United States, which is the so-called special relationship. Lot of these things, when you start sharing intelligence are person to person things, but you have that high level of trust, you see the same people same events, you might even have a little coffee group, but with a bigger organiser that's quite easy for us, because we have the Five Eyes and we will share stuff[redacted]

It's more difficult for the EU I think, because culturally, we all speak English in Five Eyes, and we've all got sort of fairly common groups and so on. Maybe more difficult to put together that higher baseline from where you start inside the European Union. These are different cultures, different languages, people you've not met before, especially if it's a very big gang of 27 or so. How will you actually end up with that proper personal trust? I once did a large-scale operation with the London special metropolitan police. This was to wind up a cyber gang, a very capable cyber gang. And the idea was to do a simultaneous arrest operation in Lithuania, Germany, Czech Republic, United Kingdom and America, simultaneously arrest them. We've all got to knock on the door and say play. So, we had, for millions and millions of pounds per year, these kinds of breakout rooms, so you have the main centre, where you do all the coordination, but of course people want to go wander off and talk to their own authorities. You must respect that. And the Americans came over and they brought the FBI and along with them was the Secret Service. And we had to give them each, the Secret Service and the FBI, a separate room, because they wouldn't talk to each other. They didn't wouldn’t work with each other, the American side was just so bleak and difficult, you had to talk to them individually.

Anyway, we got the gang in the end and brought it down but it's about the culture, and when you've got a very large number of nations, how do you bond? You gotta have the same people that we have in the virtual task forces in the financial services in the UK, in the end it's absolutely about people. If you have the same person at the top, we are all talking about the same management, John can create an earnings per share and so on, but you don't just go and say: Could you go along and have a chat with this person? It has to be the people.

I don't know what happens between GCHQ and ENISA, I'm afraid. For example, one would hope that old friendships and old routes to communicate are still there. Why wouldn't they? Because, if they're not, then it's stupid [redacted]. The answer is, I believe in the UK we are making progress, and this is just by raising awareness of cyber security, and we have our own specific cell inside our national security agencies, who look after the space sector. The space sector is now part of the critical national infrastructure because it feeds so many other parts of it. It was only a few years ago that it was made a critical national infrastructure. So, our cooperation is getting better, it's all about getting the message to the right part of the organisation at the right time in their growth. I would hope that there is more cooperation as I say I don't know what's going on behind the scenes, a lot of this will be sort of highly classified, you gotta have a permit to get into the car park and all that kind of stuff.

The answer to *Q7* is, yes, we have been developing, what is the public-private cooperation existing space intelligence sharing and we do actually have a formal platform, our National Cyber Security Centre, which is the public-facing side of GCHQ and I've known NCSC from the very beginning, where all desks were empty, and they were about three people. Now it is absolutely humming, and they are all working on the same messages, their public information stuff is really getting quite good from a shaky start. So, in the public area, look at NCSC and how it does its work and of course it works from boardroom level down to your techie with the soldering iron - if that's what they do these days. [redacted]