TALLINN UNIVERSITY OF TECHNOLOGY
School of Business and Governance
Department of Law

Kadri Bussov

CYBERSECURING EUROPEAN UNION SPACE ASSETS

Master Thesis
Program of International and European Union Law

Supervisor: Katrin Nyman-Metcalf, PhD, TalTech University
Co-supervisor: Percy J. Blount, PhD, University of Luxembourg

Tallinn 2021

I hereby declare that I have compile the thesis independently
and all works, important standpoints and data by other authors
have been properly referenced and the same paper
has not been previously presented for grading.
The document length is 17242 words from the introduction to the end of the conclusion.

Kadri Bussov.....................................
(signature, date)
Student code: 191768HAJM
Student e-mail: bussov@gmail.com

Supervisor: Katrin Nyman-Metcalf, PhD:
The paper conforms to requirements in force

....
(signature, date)

Co-supervisor: Percy J. Blount, PhD
The paper conforms to requirements in force

6 May 2021

Chairman of the Defense Committee:
Permitted to the defense

....
(name, signature, date)

Table of Contents

Abstract

Cybersecurity on space assets is not regulated within the EU. Similarly, there are no industry-wide accepted standards for different aspects of space systems. That has led to a situation where cybersecurity on different parts of a space system is uneven. However, the convergence of different technologies brought about the rapid development of the ICT industry has created a situation where space is becoming increasingly ingrained with critical infrastructure. This thesis is conducting a legal analysis on the effects of two proposals by the European Commission on cybersecurity on critical infrastructure within the EU, including space as a sectoral scope. These Directives are a proposal for the NIS 2 Directive and a proposal for the RCE Directive. The proposals for the NIS 2 and the RCE directives do not define space in itself but through its interoperability with other sectors. The different EU regulations governing space differentiate between four areas of space and set different legal requirements for governance and cybersecurity. The TFEU separates national and EU space programs through parallel competency and grants the EU the measures to implement its space program, which it did by the agreement to establish the Union Space Program that consists of EGNOS, Galileo, Copernicus, SST, and GOVSATCOM. The TFEU exempts the EU from adopting harmonizing legislation over national space programs of the Member States. The proposals for the NIS 2 and the RCE Directives establish an area of the space that is an element of critical entities, regardless, whether they are public or private entities in nature. Furthermore, the final area is private companies that fall outside of the previous description governed by any specific EU legislation. This differentiation and multitude of legal frameworks governing space create a complex legal landscape and the definition of space and whether it falls under which EU legal framework is open for interpretation.

Keywords: *space systems, cybersecurity, critical infrastructure*

List of abbreviations and symbols

AOCS – Altitude and Orbital Control System

APT – Advanced Persistent Threat

COTS – Commercial Off the Shelf

CME – Coronal Mass Ejection

DEFIS - Directorate-General for Defense Industry and Space

ECI – European Critical Infrastructure

EDA – European Defense Agency

ENISA – European Union Agency for Cybersecurity

EGNOS - European Geostationary Navigation Overlay Service

EuroQCI – European Quantum Communication Infrastructure

EUSPA – European Union Agency for Space Program

ESA – European Space Agency

EO – Earth Observation

EWAN – EGNOS Wide Area Network

GEO – Geostationary Orbit

GNSS – Global Navigation Satellite Service

GMES - Global Monitoring for Environment and Security

GOVSATCOM - Governmental Satellite Communications

GPS – Global Positioning System

GSA – European Global Navigation Satellite System Agency

ICT – Information Communication Technology

MCC – Mission Control Center

NASA – National Aeronautics and Space Administration

NLES - Navigation Land Earth Station

NRT – Near Real Time

OST - Treaty of Principles Governing the Activities of States in the Exploration of Outer Space, including the Moon and Other Celestial Bodies

PRS - Public Regulated Service

PUA – Potentially Unwanted Application

RIMS - Ranging Integrity Monitoring Stations

RCE – Resilience of Critical Entities

SAB - Security Accreditation Board

SME – Small and Medium Size Enterprise

SST – Satellite Surveillance and Tracking

TFEU - The Consolidated Version of the Treaty on the Functioning of the European Union

TCP/IP – Transmission Control Protocol / Internet Protocol

TT&C – Telemetry and Tracking Control

WANK – Worms Against Nuclear Killers

I. Introduction

Space domain and cybersecurity are, after an initial observation, two very different domains. Yet, one could claim that the domain of cyber is overarching and swallow space in itself due to digital technology. Blount refers to space objects as mere `things within the internet of things` and describes the transformation as `satellites that were once the backbone of global connectivity are now accessible by global connectivity`.[1] The cybersecurity of satellites was once considered redundant as it was believed that satellite systems were too advanced and obscure to be hacked.[2] There is, however, plenty of evidence of the contrary. In 1998 a US-German ROSAT satellite was rendered useless when a group of hackers took control of the satellite and changed its orbital position in a way that damaged its operational instruments.[3] Cyberattacks on space systems reach even further back with one of the earliest attacks, the WANK worm attack, taking place in 1989 against Goddard Space Flight Center. The aim of the WANK worm was to disrupt the Galileo satellite launch as an activist act against nuclear weapons.[4] With the emergence and development of transmission control protocol and the internet protocol (TCP/IP) technology, cyberattacks have become more sophisticated, more common, and moved from hacktivism to state-sponsored cyberattacks. State-sponsored cyberattacks are often used as a part of hybrid war-fares waged between states for geopolitical gain.[5] This evolution in cyberattacks, together with increased dependence on space technology for critical infrastructure, makes protecting satellites from cyberattacks a vital security issue to address. [6]

Space assets are becoming increasingly more central in providing services for different industries and critical infrastructure.[7] Space-based assets are critical in providing communication, GPS, and weather data. The EU has invested heavily in developing EU

[1] Blount, P.J., 2017. Satellites are just things on the internet of things. *Air and Space Law*, *42*(3).
[2] Falco, G., 2018. The vacuum of space cyber security. In *2018 AIAA SPACE and Astronautics Forum and Exposition* (p. 5275).
[3] Fritz, J., 2013. Satellite hacking: A guide for the perplexed. *Culture Mandala*, *10*(1), p.5906.
[4] Thomas, J., 2001. Ethics of Hacktivism. *Information Security Reading Room*, *12*.
[5] Aziz, A., 2013. The evolution of cyber attacks and next generation threat protection. In *RSA conference*.
[6] Falco (2018), *supra nota*, 2, 2.
[7] Unal, B., 2019. *Cybersecurity of NATO's Space-based Strategic Assets*. Chatham House. The Royal Institute of International Affairs, 3.

capabilities through EGNOS,[8] Galileo satellite navigation system, [9] and Copernicus Earth observation constellation.[10] The latest European initiative, including space element, is the planned development and future launch of the European Quantum Communication Infrastructure (EuroQCI) as part of the GOVSATCOM space program, that sees one of its goals to improve the European satellite communication cybersecurity capabilities for both terrestrial and space domains.[11] The EU has invested and continues to invest heavily in developing the EU capacity in space with its programs for navigation, Earth observation, communication, and space situational awareness.

The cybersecurity issue became especially relevant in 2019, where the world saw the emergence and spread of a new highly infectious disease, Covid-19. In order to combat the disease, many countries implemented nationwide lockdowns to slow the spread of the virus. These lockdowns resulted in implementing remote working regimes where employees switched to using predominantly digital tools to conduct their work tasks and keep in contact with their co-workers.[12] The Covid-19 and the resulting lockdowns further caused the migration of many services and operations to online which brought new challenges to cybersecurity.[13] The Covid-19 crisis has given the cybersecurity measures of the TCP/IP technology a serious stress-test, and exposed vulnerabilities in communication and teleconference software (Zoom bombing), increase spread of spyware, malware, and phishing attacks on healthcare systems intensified, and service outages spiked to name just a few of the emerged challenges.[14]

The European Union responded to the increased cybersecurity challenges with the collection of proposals for new Directives aimed at expanding the European resilience in infrastructures experiencing increased stress due to a networked world. In December 2020, two proposals

[8] Commission Proposal (EC) for Regulation of the European Parliament and of the Council establishing the Space Programme of the Union and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013, (EU) No 377/2014 and Decision 541/2014/EU, 2018/0236 (COD), 1.

[9] *Copernicus Overview,* European Space Agency. Retrieved from https://www.esa.int/Applications/Observing_the_Earth/Copernicus/Overview3, March 10, 2021.

[10] European Space Agency, *supra nota*, 9.

[11] *The Future is Quantum: EU countries plan ultra-secure communication network.* European Commission, Retrieved from https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network, March 10, 2021.

[12] Wang, B., Liu, Y., Qian, J. and Parker, S.K., 2021. Achieving effective remote working during the COVID-19 pandemic: A work design perspective. *Applied psychology*, *70*(1), pp.16-59., 17.

[13] Weil, T. and Murugesan, S., 2020. IT Risk and Resilience-Cybersecurity Response to COVID-19. *IT Prof.*, *22*(3), pp.4-10., 5.

[14] Weil, T. and Murugesan, S., (2020), *supra nota* 13, 7-8.

relevant to cybersecurity and space were introduced – the proposal for the Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (Proposal of NIS2 Directive)[15] and the proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities (Proposal of RCE Directive)[16]. These proposals pose new and updated cybersecurity requirements for a wider range of industries that were previously excluded and, for the first time, also include the space sector as an element of the critical infrastructure.

The inclusion of space as critical infrastructure in the proposed NIS 2 and RCE Directives creates tools needed to harmonize the legislation on space systems on the aspects that are most relevant to the EU by including space as a critical entity. However, the proposal of the NIS 2 Directive does not specify or define what it means by "space" in the context of the proposal and instead leaves the interpretation open to the Member States.[17] The Proposal of the RCE Directive is a complementary proposal to the Proposal of the NIS 2 Directive in the area of identifying and designating European critical infrastructures and assessing their need for protection.[18] In order to assess the proposed cybersecurity measures implemented by the EU in protecting its space assets, both proposals should be viewed in unison in the context of competencies described in the Treaty on the Functioning of the European Union (TFEU).

The purpose of this thesis is to understand the urgency and probability of cyberattacks on the European Union space systems and to answer the question of whether including space as critical infrastructure in the proposals for NIS 2 and the RCE Directive is justified. The research questions for this thesis are (1) how much of the EU space systems and space industries fall under the scopes of proposed NIS 2 and RCE Directives and (2) to analyze the effect of legal requirements for security-by-design and of resilience policies on EU space system.

The thesis uses different methodologies in the research of its question. The primary methodology used is qualitative with legal analysis on specific issues on the EU law. The thesis also relies heavily on comparative methodology between practical use-cases and proposed

[15] European Commission (EC), *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.* Brussels, 16.12.2020.
[16] European Commission (EC), *Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities.* Brussels, 16.12.2020.
[17] European Commission (EC), *supra nota,* 15, 34. (NIS2)
[18] *Ibid.*, 3.

policies. As cybersecurity is a multi-disciplinary field with a firm reliance on the technology sector, the thesis will also analyze technical aspects as far as is necessary. Space, similarly, is a highly technological field as for which reason analyzing technological aspects of space systems is necessary. The analysis conducted is a legal analysis.

A large portion of the thesis will be dedicated to different technical solutions as both cyberspace and space are technology-heavy industries. The human capabilities to act in any particular way within these domains are dictated by technological capabilities. The underlying technical code or the software is determining what is possible in cyberspace. Software regulates behavior online in a similar manner as laws of physics regulate behavior in the natural world.[19] In order to implement any action, the implementer needs to follow the technical codes of cyberspace or rather the actions within the cyberspace follow the pre-determined rules of the cyberspace, and the software code acts as a law regulating cyberspace.[20] Similarly, human space capabilities are dictated by our technical capabilities and available engineering solutions.

The thesis is divided into three chapters. The first chapter gives an overview of the development of space in Europe and a short history of the creation of the Galileo, Copernicus, and EGNOS programs. It will explain the TFEU Article 189 and Article 4 (3) and the limitations and parallel competencies it creates in the area of space. The first chapter will also look at the Strategy of Space for Europe and how the priorities and activities described in it creates content in understanding the meaning of "space" within the EU. The chapter will not try to define "space" but merely acknowledges the lack of an internationally accepted definition for it and how the Space Strategy for Europe uses describing activities in creating substance for the term "space". The first chapter will not look at the relationship between cyber and space beyond what is indicated in the Space Strategy for Europe but instead focuses on giving the reader a foundation for understanding the context of space within the EU.

The second chapter focuses on the different legal frameworks governing the security of the EU space sector and is divided into three subsections. The first subsections will focus on the EU Space Program and the role of the security accreditation board in providing cybersecurity standards and oversight of the EU space programs Galileo, EGNOS, Copernicus, SST, and

[19] Lessig, L., 2009. *Code: And other laws of cyberspace*. ReadHowYouWant. com, 10.
[20] Grimmelmann, J., 2004. Regulation by software. *Yale LJ*, *114*, p.1719., 1721.

GOVSATCOM. The thesis will not take a closer look at SST and GOVSATCOM programs as SST stands for space situational awareness for satellite traffic in the orbit, and GOVSATCOM is not yet operational. The second subchapter looks more closely at the role of the European Defense Agency in identifying cyber vulnerabilities and research and development priorities for establishing EU non-dependence within the space sector. The third subsection will focus on the inclusion of the space sector in the proposals of the NIS 2 and the RCE Directive. The main focus is on identifying the scope of space sector involvement in the EU critical infrastructure framework for cybersecurity.

The final and the third chapter will look at the potential developments of the space sector as it matures into an industry with a high number of nodes, and more companies enter as the market matures and becomes profitable. The first part of the final chapter will focus on the EU programs EGNOS, Galileo and Copernicus and will look more closely at which elements and technologies these systems are composed of. It will also look at the set-up of the system´s design from the security of design point of view and whether these systems will fall under the proposed NIS 2 and RCE Directives. The second part of the third chapter will focus on commercial actors of the space sector and look at the emergence of large – and mega – constellations developed and launched by private companies for Earth observation and communication. It will also look at how the proposed NIS 2 and RCE Directives would affect the EU companies setting out to launch satellite constellations in providing services and applications to the clients within the EU.

II. The European Union and space

II.I. Brief history of European space

The relationship between Europe and space has evolved gradually starting from the second half of the 20th century. Space became a global focus in 1957 when the Soviet Union launched the first artificial satellite, Sputnik I, and this propelled the United States and the Soviet Union into a Space Race which ended on July 20, 1969, when Neil Armstrong and Buzz Aldrin walked on the Moon. [21] During this period, many significant breakthroughs in the space sector were reached, including the first human spaceflight by Yuri Gagarin, the first mission to leave the Earth orbit, the Luna I, the first mission to reach the Moon, the Luna II, and the first mission to head towards Venus, the Venera by the Soviet Union.[22]

In the European region, the first states to make investments in the space sector were France, Italy, and the United Kingdom in the 1950-s. [23] In the 1960-s, however, the first initiatives led by scientists and the Member States emerged. The European Preparatory Commission for space research gave rise to ten European states establishing the European Space Research Organization and European Launcher Development Organization, which led to the creation of the European Space Agency (ESA) on 30 May 1975.[24] The European Space Agency, or ESA for short, is an operational intergovernmental organization which mandates derive from the Convention of the European Space Agency.[25]

In the 1980-s, the first space policy was adopted by the ESA. The ESA was the main leading force in the European space sector during the 1980-s, while European Commission and the Council played a minor role. In the 1990-s, the European Commission and the European Council moved towards taking up more of an active role.[26] This development led to the creation of the European Commission starting to develop stronger links and collaboration with ESA.[27]

[21] *What was the space race?* Space.com. Retrieved from https://www.space.com/space-race.html, March 24, 2021.

[22] *Ibib.*

[23] Reillon, V., 2017, *European Space Policy. Historical perspective, specific aspects and key challenges*. European Parliamentary Research Service, 1.

[24] *Ibid.*

[25] von der Dunk, F. ed., 2015. *Handbook of space law*. Edward Elgar Publishing, 391.

[26] Reillon, V., (2017), *supra nota*, 23, 6.

[27] *Ibid.*, 7.

The first significant space system developed in collaboration with the European Commission, ESA, and the Eurocontrol was the European Geostationary Navigation Overlay Service (EGNOS).[28] The EGNOS is a regional satellite-based augmentation system to improve the global navigation satellite service's (GNSS) performance in Europe.[29] The second significant space system that the EU initiated in 1999 was the public-private partnership to develop Galileo's European independent satellite navigation system.[30] Galileo is a European satellite navigation system that provides global positioning and is part of the GNSS system.[31] Galileo and GNSS are space systems of significant magnitude, and in order to manage and operate EGNOS and Galileo, a Community Agency was established by the Council Regulation (EC) 1321/2004.[32] The Community Agency was re-structured under the EU law into the European GNSS Agency (GSA) in 2010 and is operating as an EU body.[33]

The third significant space system initiated by the European Community in collaboration with ESA was the earth observation initiative Global Monitoring for Environment and Security (GMES).[34] To honor the European scientist Nicolaus Copernicus GMES was later renamed to Copernicus.[35] The development, design, and construction of Copernicus infrastructure is the responsibility of ESA and was funded by the European Community.[36] The Copernicus provides data on land, marine, and atmosphere, which is used to monitor climate change, manage emergency response, and other security purposes. The data collected is made available for companies to develop services and applications. [37]

[28] Reillon, V., (2017), *supra nota*, 23, 9.

[29] *What is EGNOS?*. GSA. Retrieved from https://www.gsa.europa.eu/egnos/what-egnos , March 12, 2021.

[30] Reillon, V., (2017), *supra nota*, 23, 10.

[31] *Galileo is the European global satellite-based navigation system.* GSA. Retrieved from https://www.gsa.europa.eu/european-gnss/galileo/galileo-european-global-satellite-based-navigation-system , March 12, 2021.

[32] *About GSA,* GSA, Retrieved from https://www.gsa.europa.eu/gsa/about-gsa#history, April 25, 2021.

[33] Reillon, V., (2017), *supra nota*, 23, 10.

[34] *Ibid.*

[35] *About Copernicus.* Copernicus. Retrieved from https://www.copernicus.eu/en/about-copernicus, March 12, 2021.

[36] Reillon, V., (2017), *supra nota*, 23, 1.

[37] *Ibid.*, 11.

II.II. The TFEU Article 189 and parallel competencies

The Consolidated Version of the Functioning of the European Union (TFEU) came into force on the 1st of December 2009 with the signing of the Lisbon Treaty. The TFEU introduced Article 189 that laid the legal foundation for the EU to establish the European Space Program.[38] Article 189 of the TFEU reads:

1. To promote scientific and technical progress, industrial competitiveness and the implementation of its policies, the Union shall draw up a European space policy. To this end, it may promote joint initiatives, support research and technological development and coordinate efforts needed for the exploration and exploitation of space.
2. To contribute to attaining the objectives referred to in paragraph 1, the European Parliament and the Council, acting in accordance with the ordinary legislative procedure, shall establish the necessary measures, which may take the form of a European space program, excluding any harmonization of the laws and regulations of the Member States.
3. The Union shall establish any appropriate relations with the European Space Agency.
4. The Article shall be without prejudice to the other provisions of this Title.

Article 189 establishes a framework for the EU to approach space policy within its jurisdiction. Article 189 establishes the EU priorities regarding space, measures the EU can take to achieve these goals, and legal restrictions stemming from Article 4 (3), which states that *in the areas of research, technological development, and space, the Union shall have competence to carry out activities, in particular to define and implement programs. However, the exercise of that competence shall not result in Member States being prevented from exercising theirs.*

Article 189 (1) establishes the aim of the European space policies to promote scientific and technical progress, industrial competitiveness, and the implementation of its policies in these areas. Article 189 (1) additionally grants the EU competence to undertake joint initiatives and coordinate activities on space exploration and exploitation.

[38] Reillon, V., (2017), *supra nota*, 23, 14; *Treaty of the Functioning of the European Unio.* Eurofund. Retrieved from https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/treaty-on-the-functioning-of-the-european-union, March 11, 2021.

Article 189 (2) establishes the legal measures the EU can take in order to achieve the goals of the European space program, one of them being the establishment of the European space program. Article 189 (2) also institutes the limitations to the legal tools the EU can use to implement its space policies. Article 189 (2) introduces what is referred to as parallel competence.[39] The parallel competence stems from the legal situation in where the Member States have the competence to adopt national space policies according to their vision, as is established by Article 4 (3) of the TFEU. Article 189 (1) grants the EU the competencies to establish separate space policy for the Union and grants the EU legal measures in doing so. Article 189 (2) exempts the EU from adopting harmonizing regulation, which creates a situation where the EU can establish its priorities and space program and the Member States can establish their own and, in all things considered, these two do not have to be compatible. Article 189, however, paragraph two does not restrict the creation of other types of measures for the EU to achieve the goals set for its space policy.[40]

Article 189 and Article 4 (3) of the TFEU talk about space in an ambiguous term. Article 4 (3) sets space in the same line as research and technological development, granting the EU and the MS an equal competence to implement and define programs as they see fit. The TFEU, however, does not define the content of space in Article 4 (3). Article 189 does describe in more detail of activities the EU can do and which activities the EU is restricted to do in the space sector. Article 189, however, does not expand on the legal definition of the subject matter it is regulating.

The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including Moon and Other Celestial Bodies (The Outer Space Treaty), refers to space as outer space, including Moon and other celestial bodies, and uses the phrasing throughout its text when referencing any activities, obligations or restrictions of states to follow in their exploration and exploitation of "space". The interpretation of space in The Outer Space Treaty is through its physical location and somewhat agreed on the measurable boundary between airspace end and space.[41] There are altogether five international treaties governing different aspects of space activities. These treaties are The Outer Space Treaty, the Agreement on the

[39] von der Dunk (2015), *supra nota*, 25, 257.
[40] *Ibid.*
[41] Oduntan, G., 2003. The Never Ending Dispute: legal theories on the spatial demarcation boundary plane between airspace and outer space. *Hertfordshire Law Journal*, *1*(2), pp.64-84, 64.

Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (The Rescue Agreement), the Convention on International Liability for Damage Caused by Space Objects (The Liability Convention), the Convention on Registration of Objects Launched into Outer Space (The Registration Convention), and the Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (The Moon Agreement). The Liability Convention differentiates between outer space, airspace, and the surface of the Earth based on the physical location of where the damage occurs. The Liability Convention differentiates between damage caused to an airplane in flight, to a satellite in orbit, or on the surface of the Earth. Similarly, the Registration Convention deals with space objects and their elements through the destination of its launch. Article II defines a space object as an object launched either to Earth orbit or beyond. The Moon Agreement addresses physical celestial bodies located in outer space. With the exemption of the Rescue Agreement that addresses issues regarding astronauts in distress, the international treaties governing different aspects of space activities address space through its physical location.

Oduntan argues that states should not base their regulation on space based on its physical location but rather base it on the activities taken regardless of the specific location of these activities, and the outer space should be defined based on the concept of space activities.[42] Article 189 of the TFEU defines space through restricted and allowed activities. It leaves the content of these activities to be defined by the Member States or the EU based on their policies. On their website for Horizon funding for space, the focus of the EU space research is to foster a cost-effective, competitive and innovative space industry.[43] The definition of what is considered "space" under TFEU Article 4 (3) and Article 189, to which the parallel competence applies, could be interpreted through EU documents about space.

[42] Oduntan, G., (2003), *supra nota*, 41, 69.
[43] *Internal Market, Industry, Entrepreneurship and SMEs. Space Research*, European Commission, Retrieved from https://ec.europa.eu/growth/sectors/space/research_en , April 25, 2021.

II.III. The four priorities of the Space Strategy for Europe and how it creates the content for defining "space" in the EU

As mentioned in the previous chapter, space is not defined in the TFEU Articles 189 or 4 (3) that set restrictions and regulations on activities regarding space. The question of defining space is long-standing and has been a source of dispute since the adoption of the Outer Space Treaty.[44] In many instances, the definition of space is interpreted through its physical location and in trying to understand from where space begins. Therefore, any activities happening beyond the point considered as outer space are space activities.[45] There are more instances in where space is defined rather through the activities conducted.[46]

In 2016 the European Commission revealed the Space Strategy for Europe to better harness the benefits offered by different space applications and activities. Within the Space Strategy for Europe, space is not defined but instead described through different priorities and activities and their interactions with other sectors within the EU. The Space Strategy for Europe sets and describes four main goals.[47] When considering that "space" is defined by activities conducted, the four goals of the European Strategy for Space should help to give a context of how "space" is defined within the EU.

The first focus of the Space Strategy of Europe is on society and economy. The first goal of the Space Strategy of Europe takes advantage of the EU established space programs Galileo, EGNOS, and Copernicus.[48] The Space Strategy correctly predicts higher interoperability of different data and services provided through the flagship space systems in Europe. The Space Strategy for Europe sets ambitious goals for its three main space assets in facilitating economic prosperity and social change. The Space Strategy for Europe proposes regulatory measures in expanding markets that could benefit from the Galileo navigation system to include mobile phones, European critical infrastructure, aviation, and new chipsets and receivers sold on the

[44] Kopal, V., 1980. The Questions of Defining Outer Space. *J. Space L.*, *8*, p.154, 154.
[45] Cheng, B., 1983. The legal status of outer space and relevant issues: Delimitation of outer space and definition of peaceful use. *J. Space L.*, *11*, p.89, 89.
[46] *Ibid.*, 98.
[47] European Commission, (EC) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Space Strategy of Europe. Brussels. 26.10.2016,* 3.
[48] European Commission (EC), *supra nota*, 47, 4. (Space Strategy)

European market should be Galileo and EGNOS compatible.[49] This should lead to a higher number of consumer applications that exploit the EU-s satellite navigation capabilities.

The European Strategy for Space predicts a more robust connection of space to other areas of European strategies in the future and proposes to undertake standardization measures and create roadmaps to greater integration.[50] Earth observation data is often used to connect other data sources for creating new innovative solutions and exploit the full range of possibilities space data provides. For this purpose and to simplify access to space data, the EU should develop a digital research infrastructure for earth observation data that will exploit the benefits of the European cloud initiative.[51] In order to create stability in the space service sector that utilizes Galileo, EGNOS, and Copernicus data, the EU pledges continuous investment and further development of its flagship space programs.[52]

The priorities EU sets for the commercial and social aspect show a clear direction in more interconnections between sectors and services and the desire to exploit space applications to its full extent in Europe. The Space Strategy for Europe also points out in its action plan for the first focus area to expand on its space programs based on emerging needs, particularly in the areas of climate change and sustainable development and security and defense.[53] The first goal of the European Strategy for Space defines space through the already established space programs EGNOS, Galileo, and Copernicus and their different applications. Furthermore, it foresees the emergence of the interconnected and dependent nature of different modern technologies to which space element is part.

The second priority set by the Space Strategy for Europe addresses the global space market and European position. The Space Strategy for Europe recognizes the changing landscape of the space industry market, the increase of privately funded companies, and the emergence of NewSpace.[54] NewSpace is a term commonly used to describe the emerging space industry segment that acts similarly to the start-up scene.[55] The Space Strategy for Europe addresses the

[49] European Commission (EC), *supra nota*, 47, 3. (Space Strategy)
[50] *Ibid.*, 3.
[51] *Ibid.*, 4.
[52] *Ibid.*, 5.
[53] *Ibid.*, 5.
[54] European Commission (EC), *supra nota*, 47, 6. (Space Strategy)
[55] *NewSpace: The Emerging Commercial Space Industry*. NASA. Retrieved from https://ntrs.nasa.gov/api/citations/20160001188/downloads/20160001188.pdf, March 26, 2021.

vulnerable position the European space industry is in due to the high dependence of global supply chains and non-European origin of critical components and technologies.[56] The second priority involves creating greater synergies for research and development on a wide range of areas within already existing critical areas for the space industry and to increase the spin-in/out surface for other sectors.[57] The Space Strategy for Europe sets out to support hubs that bring together space, digital, and user sectors.[58] The intention is to foster non-space industries to exploit the application and opportunities provided by the space sector and create interconnected synergies to other sectors.[59] The second goal of the Space Strategy for Europe defines space through the desire to move towards higher digital cross-sectoral dependence between space-based elements and the private sphere. The definition of space through activities in the first and the second priority has an overarching common denominator: interoperability and embedment with other sectors.

The third focus of the Space Strategy addresses the autonomy, security, and safety aspects of the European space sector.[60] The main concern addressed by the third focus of the Space Strategy is Europe´s autonomy in accessing space. The issue is ever more pressing considering the lack of spaceports within the European territory and the dependence of the only spaceport under French jurisdiction located in French Guiana.[61] The EU intends to support the development and creation of European launch infrastructure facilities in collaboration with ESA and Member States.[62] The second objective under autonomy, security, and safety focus is the access to and the security of the radio frequency spectrum.[63] Access to and the security of the radio frequency spectrum is relevant to a wide range of commercial and government applications for both space-based systems and terrestrial-based systems.[64] However, the objective that is most relevant from the cybersecurity perspective is the objective of ensuring the protection and resilience of critical European infrastructure and reinforcing synergies

[56] European Commission (EC), *supra nota*, 47, 5. (Space Strategy)
[57] *Ibid*, 6.
[58] *Ibid*, 7.
[59] *Ibid.*
[60] *Ibid.*, 8.
[61] *Europe's Spaceport.* European Space Agency. Retrieved from https://www.esa.int/Enabling_Support/Space_Transportation/Europe_s_Spaceport/Europe_s_Spaceport2, April 11, 2021.
[62] European Commission (EC), *supra nota*, 47, 9. (Space Strategy)
[63] *Ibid.*, 9.
[64] *What is Spectrum? A Brief Explainer.* CTIA. Retrieved from https://www.ctia.org/news/what-is-spectrum-a-brief-explainer, March 26, 2021.

between civil and security space activities.[65] Providing resilience for critical European infrastructure can be achieved by approaching the issue from different aspects. One aspect is developing a more resilient satellite communication service which is built by the principle of security-by-design.[66] Another is in including space systems as critical infrastructure to provide additional requirements in securing their resilience from cyber threats. The Space Strategy does not address the latter. Nevertheless, this development was introduced in 2020 with the EU's Cybersecurity Strategy for the Digital Decade that includes space as potentially critical infrastructure for Europe.[67] In the third goal in the Space Strategy for Europe, we can see a clear indication that following through with the first two goals will raise the need for more robust measures in securing the space-based elements against cyber intrusions.

The fourth and final focus of the Space Strategy addresses Europe´s global role in the space sector and promotes furthering international cooperation in this area.[68] Space is a global field with many technological breakthroughs stemming from international cooperation and partnerships. Furthermore, the Commission plans to exploit its trade policy instruments and economic diplomacy to increase European space clusters and SME-s access to international space markets.[69]

Priorities within the Space Strategy for Europe approaches defining space through priorities that intertwine between different sectors and industries. When the Outer Space Treaty Defines space as outer space, including Moon and other celestial bodies, the Space Strategy for Europe defines space through its interaction with other industries and dedicated programs. The relevance of giving space interoperable content infuses the necessity of including space as part of different systems, including critical infrastructure.

The EU is still restricted by the TFEU Articles 4 (2) and 189 in adopting harmonizing regulations on space. Reading the wording of Article 189 (2) in the allowed measures for the EU to establish an EU space program and the continued wording for exclusion of harmonizing legislation right after it, one could interpret it as excluding adopting EU-wide harmonizing

[65] European Commission (EC), *supra nota,* 47, 9. (Space Strategy)

[66] European Commission, (EC) *Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade. Brussels. 16.12.2020,* 8.

[67] *Ibid.*, 1.

[68] European Commission (EC), *supra nota,* 47, 11. (Space Strategy)

[69] *Ibid.*

regulations pertaining to space programs. Article 4 (3) similarly mentions space programs but not space. This interpretation might leave the door open for harmonizing legislation on other aspects of space not described as space programs but defined by the activities undertaken by the EU as described in the four priorities of the European Strategy that are not considered the EU flagship space programs.

III. Creating an EU framework for cybersecurity on space assets

III.I. The European Union Space Program and the security accreditation board

In its report regarding the security of EU space assets from 2015 based on Space and Security task force that convened between September 2015 and June 2016, two potential ideas were proposed for ensuring the security of European space assets – the creation of a common risk and resilience assessment methodology for European space assets and exploiting already existing critical infrastructure frameworks for EU and on the Member State level.[70] The proposal for establishing the space program for the EU and the EU Agency for the Program creates independent risk assessment measures in its proposed Chapter II of Title V and proposals of NIS 2 and RCE Directive include space into already existing critical infrastructure frameworks. The thesis will come back to proposals of NIS 2 and RCE Directives in later chapters and will focus on risk assessment measures in the Union Space Program in the current one.

The proposal for establishing the space program for the EU and the EU Agency for the Program was first introduced in 2018 and was reaffirmed in 2020. A political agreement between the European Parliament and the EU Member States for adopting the EU Space Program and the Agency for the Space Program was reached on December 16, 2020.[71] The developments in the space sector within the EU are still in the early stages, and the real-life implications of the proposed security measures are to reveal themselves in the coming years. That being said, the Space Program does set up several changes in the governance of the EU space programs and the creation of the Security Accreditation Board (SAB) for the EU Space Program.[72]

The idea of a SAB is not new as the GSA has been hosting an independent SAB to oversee the security-related tasks in ensuring the robustness and resilience of Galileo and EGNOS.[73] The composition of the SAB in GSA are described on their website as consisting of representatives from each MS, from the Commission, and from Union for Foreign Affairs and Security Policy. The main competencies of the SAB in GSA are to decide on the approval of the security

[70] Pellegrino, M. and Stang, G., 2016. *Space security for Europe*. EU Institute for Security Studies, 6.

[71] *Commission welcomes the political agreement on the European Space Programme.* European Commission. Retrieved from https://ec.europa.eu/defence-industry-space/commission-welcomes-political-agreement-european-space-programme-2020-12-16_en, March 29, 2021.

[72] Commission Proposal (EC), *supra nota*, 6, 47. (Space Program)

[73] *Security*, GSA, Retrieved from https://www.gsa.europa.eu/about/what-we-do/security, April 24, 2021.

accreditation strategy, to authorize the launch of satellites, on whether to change the configurations of already operational systems, to authorize whether to operate a ground station and whether to manufacture receivers containing public regulated service (PRS) technology and their components.[74] The GSA, as mentioned earlier is the EU agency that is responsible for the governance of the EGNOS and Galileo space systems.

Article 1 (2) of the Proposal for the EU Space Program and the Agency for the Space Program establishes that the GSA will become the EU Agency for Space Program.[75] Article 3 establishes the five elements of the European Space Program: Galileo, EGNOS, Copernicus, space surveillance, and tracking (SST) and governmental satellite communications service (GOVSATCOM).[76] The responsibilities of the GSA will be significantly expanded by the adoption of the EU Space Program. The Proposal for the EU Space Program and the Agency for the Space Program will, in addition, significantly expand and clarify the role of the SAB.

The Title V of the proposal of the EU Space Program and for the Agency for the Space Program is dedicated to the security of the Space Program. Title V is named Security of the Program and consists of three chapters and nine articles. The relevant articles pertaining to the security governing the current GNS agency were set up in Articles 10 and 11 of Regulation (EU) No 912/2010 of setting up the European GNSS Agency.

In Article 34 (1), the security priority of the Space Program is stated as the protection of infrastructure, both ground and space, and the provision of services, particularly against physical and cyber-attacks.[77] Article 34 (3) and (4) divide security responsibilities between the Agency and the Member State. Article 34 (3) (a) poses the responsibility to ensure the security accreditation of all components of the Union Space Program are in accordance with the Chapter II of Title V and further poses an obligation to ensure competencies of the Member State. Article 34 (2) states that *the entity responsible for the management of a component of the Program shall be responsible for managing the security of that component and shall, to that end, carry out risk and threat analysis and all the necessary activities to ensure and monitor the security of that component, in particular setting of technical specifications and operational*

[74] GSA, *supra nota*, 73.
[75] Commission Proposal (EC), *supra nota*, 8, 31. (Space Program)
[76] *Ibid.*, 33.
[77] *Ibid.*, 33.

procedures, and monitor their compliance with the general security requirements.[78] The component of the EU Space Program is not the same as the element of the EU Space Program. A single element of the EU Space Program can consist of several different components such as satellites, ground stations, data collections, and many more, which can be managed and operated by different entities.[79]

The proposal for the EU Space Program Article 35 states that the SAB established within the Agency shall be the security authority for all of the components of the EU space program.[80] A notable difference between the SAB in the GSA and the SAB described in the Proposal for the EU Space Program is its decision-making process. The SAB in the GSA is obliged to address their decisions to the Commission as per Article 11 (6) of Regulation (EU) No 912/2010. The decisions made by the SAB per the Proposal for the EU Space Program should be reached by consensus, and the decisions of the SAB are made in the context of collective responsibility of the EU and the Member State.[81] The SAB described in the EU Space Program is similarly obliged to address their decisions to the Commission. However, collective responsibility and consensus-based decision-making could result in significant disadvantages in the effectiveness of the SAB. Article 36 (b) states that *efforts shall be made for the decisions within the SAB to be reached by consensus.* The linguistic interpretation of this clause does leave room for decisions to be made without necessarily reaching consensus, but the clause does not indicate in which situations these exemptions can be done. Whether the decision-making process favoring consensus and the resulting MS responsibility cause delays in the decision-making process is yet to be foreseen. The tasks under SAB for which the decisions pertain are described in Article 37.

Article 37 (2) imposes the following tasks to the SAB: (a) defining and approving a security accreditation strategy setting out; (b) taking security accreditation decision, in particular on the approval of satellite launches, authorization in operating programs, changing configuration; (c) examining and approving documentation relating to security accreditation; (d) advising Commission on issues in their competence; (e) examining and approving security risk assessments; (f) checking the implementation of security measures; (g) endorse approved

[78] *Ibid.*
[79] *Ibid.,* Full text.
[80] *Ibid.,* 33.
[81] *Ibid.,* 34.

products and measures which protect against electronic eavesdropping and of cryptographic products; (h) approve the interconnection of products and services; (i) agreeing with MS over the template for access control measures; (j) preparing and informing Commission of the risk reports; (k) assisting the Council and High Representative; (l) carrying out consultations which are necessary to perform its tasks; (m) adopting and publishing rules.

The list composed in Article 37 (2) is exhaustive and describes the tasks of the SAB in ensuring the security of the EU Space Program and its elements. Article 34 (4) (b) poses an obligation to the Member States to perform security accreditation tasks described in Article 41. Under the authority of Article 41, each Member State should transmit to the SAB all information they consider relevant for the purposes of security accreditation under their jurisdiction. The SAB aims to manage risks posed on space assets through inspections, audits and tests.[82] These principles highlight the need to assess the resilience of relevant systems located in a Member State jurisdiction and ensure that access control to similar systems across all the Member States has the same level of security.[83] These requirements follow two main cybersecurity principles of security-by-design and resilience of systems.[84]

The inclusion of cybersecurity as a security priority in Article 34 (1) creates a situation where security issues pertaining to cybersecurity fall under the authority of SAB. Gregory Falco has pointed out as one of the main issues with cybersecurity on space assets is the lack of standards and regulations.[85] The EU Space Program Title V creates standards and regulations to govern security issues on the space elements falling under the EU Space Program. As is set in Article 1 (2), these elements are Galileo, EGNOS, Copernicus, SST, and GOVSATCOM. The TFEU Article 189 (2) excludes the competence of the EU to adopt EU-wide harmonizing legislation regarding space programs and space policies that fall outside the EU’s own space programs and policies. Therefore, the SAB authority and the security measures described in Title V will not apply to other space systems operated and developed within the EU.

[82] Commission Proposal (EC), *supra nota*, 8, 86. (Space Program).
[83] *Ibid.*, 87.
[84] Anderson, R., 2020. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons, 8.
[85] Falco, G., 2019. Cybersecurity principles for space systems. *Journal of Aerospace Information Systems*, *16*(2), pp.61-70, 62.

III.II. The role of EDA in defining critical European space elements

III.II.I *Strategic Context Cases*

The European Defense Agency (EDA) was created on the 12th of July 2004 with the European Council formally adopting Joint Action, and therefore the EDA was established.[86] The significance of the EDA when talking about the space sector and its security within the EU stems from its mission to support and develop the EU defense capabilities, including capacity building in space and cybersecurity.[87]

The EDA has determined priority areas for the space sector in Europe to be space-based information services, information superiority, air superiority, and cyber defense in space.[88] The EDA, in collaboration with EC and the ESA, has developed a list of critical space technologies for European strategic non-dependence.[89] The European non-dependence as an objective by the EDA aligns with the third priority of the Space Strategy for Europe.

The EDA strategic context cases (CCC) identified 11 priorities divided between five domains where space and cyber are being grouped into one.[90] Their shared technical elements interconnect the identified priorities. Many identified CCC priorities share space-based capabilities for their development and operations. This approach closely resembles one taken by the Space Strategy for Europe in defining space.

The defense sector relies heavily on satellite systems for its everyday operations, making space systems subject to different cyber-attacks from adversarial nation-states.[91] Cyberattacks conducted by nation-states differ from cybercrime in their target selection, resources, and deployment of sophisticated reconnaissance and information-gathering.[92] The advance

[86] *Our History*. European Defense Agency, Retrieved from https://eda.europa.eu/our-history/our-history.html, April 27, 2021.
[87] *Mission*, European Defense Agency, Retrieved from https://eda.europa.eu/who-we-are/Missionandfunctions, April 27, 2021.
[88] *Space Fact Sheet*. European Defense Agency. Retrieved from https://eda.europa.eu/docs/default-source/eda-factsheets/2018-09-21-factsheet_space.pdf, April 1, 2021.
[89] *Ibid.*
[90] *Strategic Context Cases (CCCs)*. European Defense Agency. Retrieved from https://eda.europa.eu/docs/default-source/eda-factsheets/2019-10-25-factsheet-scc, April 1, 2021.
[91] Brenner, S.W., 2009. *Cyberthreats: The emerging fault lines of the nation state*. Oxford University Press, 105.
[92] Tankard, C., 2011. Advanced persistent threats and how to monitor and deter them. *Network security*, *2011*(8), pp.16-19, 16.

persistent threats (APT) use a multitude of tools in gaining access to the system.[93] The NSA Director of Cybersecurity, Rob Joyce, has indicated six distinctive phases used in APT. The first phase is the reconnaissance, during which social engineering is used to identify individuals to help intrude the system. During this phase, the system and its components themselves are meticulously studied. The purpose of this phase is to become a specialist in the knowledge of the system.[94] The second phase consists of initial exploitation, during which the actor tries to get into the system. The third is establishing persistence, in which stage the tools for continued presence are being implemented, expanding on the privileges the actor has in the system. The next phase is installing tools for lateral movement until finally the attacker finds and exploits the information it is after.[95] Although Rob Joyce is not addressing issues for space systems, the general structure of APT is universal and would apply to any system, including space.

Falco has addressed different attack vectors on systems in several of his articles and has pointed out that space systems are becoming increasingly more attractive targets as the interoperability between sectors grows and space systems are becoming single-point failures for other industries.[96] Deducing from the concerns voiced by Falco and considering the priorities set by the Space Strategy for Europe, the EU space assets are likely becoming convenient targets for APT´s. The attractiveness of satellites as targets for cyber-attacks grows even more when considering the increasing number of commercial satellites with lower required cybersecurity standards and the potential of using hacked satellites with propulsion systems as targeted weapons in orbit against other satellites.[97]

Protecting satellites critical for national defense and EU defense against cyber-attacks is vital for the EDA, especially as many defense capabilities simultaneously incorporate aerial, ground, and space technology. The CCC-s bring out the interoperability between EDA priorities and illustrate the dependence between them. As an example, ground combat capabilities as a priority include platforms for unmanned vehicles.[98]

[93] Tankard, C., (2011.), *supra nota*, 92, 17.

[94] *Disrupting nation state hackers.* USENIX. Retrieved from https://www.usenix.org/conference/enigma2016/conference-program/presentation/joyce, March 16, 2021.

[95] *Ibid.*

[96] Falco, (2018), *supra nota*, 2, 2.

[97] Falco, G., 2020. When Satellites Attack: Satellite-to-Satellite Cyber Attack, Defense and Resilience. In *ASCEND 2020* (p. 4014), 4015.

[98] European Defense Agency, *supra nota*, 90. (CCCs)

Precision striking is a technology that relies on a multitude of enabling technologies with guidance and control technology strongly connected to the satellite navigation capabilities. [99] Additionally, precision striking requires target recognition systems dependent on high-resolution radar data provided by overhead tactical satellites or/and unmanned air vehicles.[100] In 2011 a USA military drone was spoofed by Islamic Republic forces causing it to land on Iranian territory instead of a US-controlled military base in Afghanistan.[101] The incident illustrated the vulnerabilities of interconnected technologies and how security breach on one system can spill over into a more significant security incident.

Spoofing is considered a cyber-attack as its purpose is to manipulate the triangulation signals causing errors and cause the receiver to calculate the positioning in a way that does not represent the actual location.[102] This type of error can cause significant harm depending on the purpose of the signal is being used. For example, if spoofing is being used to interrupt Search and Rescue applications, the result can be loss of human life.

There is a well-founded reliance on space-based data for many of the priorities for the EDA. The space-based information and communication services bring out priorities for earth observation, positioning, navigation and timing, space situational awareness, and satellite communication.[103] These priorities mirror the EU flagship programs under the EU Space Program. The EDA 2020 Annual Report re-emphasizes the importance of continued execution on the CCCs.[104] The EDA, much like the Space Strategy for Europe, describes space through its interoperability with other priorities and sectors relevant for EU defense.

[99] Fleeman, E.L., 2001. Technologies for future precision strike missile systems, iii.

[100] *Ibid*, I-4.

[101] *Iran `spoofed` US drone in order to land it.* The Jerusalem Post. Retrieved from https://www.jpost.com/Iranian-Threat/News/Iran-spoofed-US-drone-in-order-to-land-it, April 2, 2021.

[102] Falco, (2018), *supra nota*, 2, 6.

[103] European Defense Agency, *supra nota*, 90. (CCCs)

[104] *Annual Report 2020.* European Defence Agency. Retrieved from https://eda.europa.eu/docs/default-source/eda-annual-reports/eda-annual-report-2020.pdf, April 2, 2021.

III.II.II. *EDA-s role in EU non-dependence in space*

The Space Strategy for Europe highlights the need for non-dependence by developing technologies within the EU and helping to secure supply chains. Complex supply chains increase the vulnerabilities of space assets.[105] Having complex global supply chains increases the number of individuals and companies involved in developing a component. This leads to uneven distribution of technical skills and security measures across the supply chain and leaves the weakest links vulnerable for attacks.[106] The Covid-19 pandemic has also shown the weaknesses of global supply chains, with many individuals taken out from the workforce and companies unable to keep their doors open due to national lockdown measures.[107] Especially vulnerable are companies that require manufacturing on-site, which is what a large part of space technology is – hardware produced on site. The Covid-19 pandemic can potentially further harm the uneven distribution quality level of specialists on a field where a skillful workforce is already causing security gaps in supply chains.[108]

In 2015, the EDA, in collaboration with ESA and the Commission, assembled a specific list of critical space technologies for European strategic non-dependence. The list contains 48 different technologies required for building and developing different subsystems of satellites and space systems.[109] Many of the technologies on the list are controlled by the International Traffic in Arms Regulation (ITAR), making the acquisition of some critical technologies complicated. The technologies that the ITAR controls are strategically relevant for the EU to develop and produce independently within the EU. The list for technologies for EU non-dependence consists of specific technologies for different elements in a space system. Some technologies are novel and are needed to execute on the priorities set in the Space Strategy for Europe.[110]

[105] Falco, G., *supra nota*, 2, 3.
[106] Khan, O. and Estay, D.A.S., 2015. Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review*, *5*(4), 1.
[107] *The new coronavirus could have a lasting impact on global supply chains*, The Economist, Retrieved from https://www.economist.com/international/2020/02/15/the-new-coronavirus-could-have-a-lasting-impact-on-global-supply-chains, April 28, 2021.
[108] Falco, G., *supra nota*, 2, 3.
[109] EC, ESA, EDA, *Critical Space Technologies for European Strategic Non-Dependence. Actions for 2015/2017 V1.16*, March 2015.
[110] *Ibid.*, full text.

Much like the EU Space Program has limited implementation when posing regulations and standards for security on space systems, the EDA is similarly limited in its scope. However, as Falco mentions, the emergence of companies launching satellites increases the attack surface for different actors seeking to cause harm.[111] The TFEU Article 4 (3) and Article 189 restrict the EU in harmonizing regulations pertaining to space programs of Member States. The interpretation of space through its interoperability with other sectors in the Space Strategy for Europe highlights how the space element is becoming a vital part of various infrastructure, including providing essential services for the EU. The EDA's relevant role in securing the EU space assets is identifying the components necessary for technology development within the EU.

III.III. Space systems as critical infrastructure under proposed NIS2 and RCE Directives

III.III.I. *Defining space systems*

Ross Anderson defines a system as:

> *`a product or component, such as cryptographic protocol, a smartcard, or the hardware of a phone, a laptop or server; or one or more of the above plus an operating system, communications and other infrastructure; or the above plus one or more applications; or any or all of the above plus IT staff; or any or all of the above plus internal users and management; or any or all of the above plus customers and other external users`*[112]

Based on the definition of a system given by Ross Anderson, space systems can be divided into sections. However, the most comprehensive definition of a system should be favored unless there is a solid reason to opt for more restrictive one.[113] Falco defines space systems through the practical pathway the different elements take, starting from planning, manufacturing, launch, and operations.[114] Falco's definition of space systems leaves room for each of the systems to have subsystems and does not contradict the system definition posed by Anderson.

[111] Falco, G., *supra nota*, 85, 2.
[112] Anderson, (2020), *supra nota*, 84, 12.
[113] *Ibid*.
[114] Falco, G., *supra nota*, 2, 4.

The Space Strategy for Europe similarly considers different aspects of space systems when defining its priorities. The Space Strategy for Europe is less structured in building up its priorities using structured systems as described by Anderson and Falco. Nevertheless, the different elements of space systems can be seen as a continuous undertone in the Space Strategy for Europe's priorities.

When considering which infrastructure servicing the space sector should be considered a critical entity, a space system should be viewed as one, and for a sustainable space market, the security of all elements of space systems should be addressed. Critical elements for space systems are launch capabilities, ground stations, and satellite manufacturing.[115] The Space Strategy for Europe predicts a higher inter- connectedness between different sectors and does not differentiate space elements from other industries. Instead, it approaches space as an interoperable element in a more extensive system.

III.III.II. *Space as an element in critical infrastructure*

The Space Strategy for Europe and the proposal for the EU Space Program intend to create more significant synergies between space and digital technologies. The high connectedness that has stemmed from ICT technology has made satellites increasingly more network compatible.[116] As was mentioned above, space systems are becoming increasingly more ingrained in other systems and technologies. The convergence of technologies with the space sector is a double-sided sword. On the one hand, it creates commercial and societal benefits and allows for the development of novel applications.[117] On the other hand, when implemented within critical infrastructure and when compromised, the same developments can cascade and cause spill-over effects to multiple essential and other sectors and services.[118]

The EU has in its toolbox the ability to implement regulatory measures to support the European space industries´ capacity to develop different space-related markets more securely. The NIS

[115] Falco, (2018), *supra nota*, 2, 2.
[116] Blount, P.J, (2017), *supra nota*, 1, 274.
[117] *Ibid.*, 279; European Commission (EC), *supra nota*, 47, full text. (Space Strategy)
[118] USENIX, *supra nota*, 94.; Falco, G., (2018), *supra nota*, 2, 2.

2 Directive and RCE Directive proposals have introduced space as an element of critical entities.[119]

The Proposal of NIS 2 revises the currently in effect Directive 2008/114/EC on the identification and designation of European critical infrastructures and assessing the need to improve their protection (ECI Directive) and its limited sectoral applicability to energy and transportation.[120] The Proposal for RCE Directive is complementary to NIS 2 Directive and increases the number of critical sectors from six to ten – energy, transportation, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, and space.[121] The Proposal for NIS 2 Directive similarly expands the list for essential sectors within the EU to include space.[122] The idea of including space elements as part of critical infrastructure has been around for a while. In 2001, several scholars pointed out the interdependencies of different critical infrastructures, which included communications satellites.[123] Among eight other sectors, communications were considered critical infrastructure by the United States (US) as early as 1997.[124] The inclusion did not *per se* stated a space as an element, but communication satellites were already in use as early as the 1960-s.[125] From this perspective, it is surprising that the EU has taken so long to implement regulations in protecting the EU space assets. Especially considering the investments and significance the EU poses on Galileo, EGNOS, and Copernicus programs.

As mentioned above, the TFEU Article 4 (3) and Article 189 restricts the EU in adopting harmonizing regulations over Member States space programs, and activity and this could have been the reason for not including space element in EU directives sooner. Including space as critical infrastructure to proposed NIS 2 and RCE Directives could create a workaround from TFEU Articles 4 (3) and 189 that would allow the EU to adopt legislation under the condition that space element regulated is part of a critical entity. The TFEU Article 4 (2) (2) grants the EU shared competencies in adopting harmonizing legislation in the area of freedom, security, and justice. The convergence of technologies made possible by the ICT/IP technology makes

[119] European Commission (EC), *supra nota*, 15, 10. (NIS2)
[120] *Ibid.*, 2.
[121] European Commission (EC), *supra nota*, 16, 3. (RCE)
[122] European Commission (EC), *supra nota*, 15, 9. (NIS2)
[123] Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE control systems magazine*, *21*(6), pp.11-25, 11.
[124] *Ibid.*, 12.
[125] Jacoby, D.L., 1960. Communication satellites. *Proceedings of the IRE*, *48*(4), pp.602-607, 603.

it possible for the EU to attempt to harmonize legislation on space in the areas that are significant and critical to the functioning of the EU as an area of freedom, security, and justice in as far they pertain to the interconnected natures of these sectors.

Including space as an essential service in the proposed NIS 2 Directive will allow for the development and implementation of higher cybersecurity standards and profiles required from the operators of space systems.[126] Many scholars have pointed out that the current situation on industry-wide or regionally implemented cybersecurity standards for space systems is severely lacking.[127] Historically, cyber-attacks on space assets were considered too difficult to execute as space systems were thought to be too sophisticated for a successful cyber intrusion.[128] The rapid development of ICT capabilities and the convergence of space to other technologies created an attack surface that previously was not present. This coupled with the advancements of cyber-attacks from hacktivism to government-funded APT's used in hybrid warfare for geopolitical gain, creates vulnerabilities to space assets.[129] The EU Space Program establishes the SAB as an authority body overseeing security measures on Galileo, EGNOS, Copernicus, SST, and GOVSATCOM programs. However, these five space systems are not the only space systems in the EU providing data and contributing to the operations of essential services and applications.

The Impact Assessment conducted prior to the proposal of the NIS Directive indicated several shortcomings on the part of the current NIS regulation in force, and the Proposed NIS 2 Directive aims to rectify these shortcomings and increase the number of cross-border services included under the regulation.[130] The currently in effect redaction of the NIS Directives´ objectives are to manage security risks, protect against cyber-attacks, better detect cybersecurity events, and minimize cybersecurity incidents.[131] However, the Impact Assessment for the NIS Directive identified a low level of cyber resilience of businesses operating in the EU, an inconsistent level of resilience across Member States and sectors, and

[126] European Commission (EC), *supra nota*, 15, 17. (NIS2)
[127] Falco, (2018), *supra nota,* 2, 3.; Falco, (2018), *supra nota,* 2, 3.
[128] *Ibid.*
[129] Blount, P.J. (2017), *supra nota,* 1, 279; European Commission (EC), *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats. A European Union response.* Brussels, 6.4.2016, 10.
[130] European Commission (EC), *supra nota*, 15, 5. (NIS2)
[131] Wallis, T. and Johnson, C., 2020, June. Implementing the NIS Directive, driving cybersecurity improvements for Essential Services. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-10). IEEE, 2.

low level of joint situational awareness, and a lack of joint crisis response.[132] The Impact Assessment results do not mention the space sector specifically but are indicative to cross-border and cross-sectoral dependence. This causes a valid concern that space systems within the EU are not sufficiently protected against cyber-attacks.

III.III.III. The different scopes of NIS 2 and RCE Directives regarding space element

Article 2 of the Proposal for the NIS 2 Directive establishes the scope of the Directive to apply to public and private entities of a type referred to as essential entities per Annex I and as important entities per Annex II. Article 2 further exempts entities that can be qualified as micro or small enterprises as per Commission Recommendation 2003/361/EC. Subsection 2 of Article 2 further gives exemptions for micro and small enterprises if the following conditions apply:

a) The services are provided by either public communications networks or publicly available electronic communication services or by providing trust services or top-level domain name registry and domain name system (DNS) service providers;
b) The entity is a public administration entity;
c) The entity is a sole provider of a service in a Member State;
d) Potential disruption of the service provided by the entity could have an impact on public safety, public security, or public health;
e) Potential disruption of the service provided by the entity could induce systemic risks, in particular for the sectors where such disruption could have a cross-border impact;
f) The entity is critical because of its specific importance at a regional or national level for a particular sector or service or other interdependent sectors in the Member State;
g) The entity is identified as a critical entity according to the RCE Directive or equivalent to a critical entity per the RCE Directive.

Regardless of its size, for a private or a public entity to fall under the proposed NIS 2 Directive scope, the entity must meet any or several of the listed requirements in Article 2 (2). The proposed NIS 2 Directive sectoral scope is stated in Annex I and Annex II of the NIS 2 Proposal. Neither of the Annexes is included with the proposal document. Nevertheless, the

[132] European Commission (EC), *supra nota*, 15, 1. (NIS2)

explanatory part of the proposal document lists the space sector as part of entities in Annex I.[133] It is to be seen how the space sector will be explained and defined in Annex I, but the requirements stated in Article 2 (2) indicate the nature of the entities falling under the scope of the proposed NIS 2 Directive.

Article 1 of the Proposal of the RCE Directive establishes the scope of the proposed RCE Directive and exempts matters covered by the NIS 2 Directive without prejudice to Article 7 of the proposed RCE Directive. Article 7 of the RCE Directive describes the identification notification of entities equivalent to critical entities. The RCE Directive poses the responsibility to take measures in ensuring the business continuation of services essential for the maintenance of vital functions or economic activities to the Member State.[134] Article 2 of the Proposal of the RCE defines "critical entity" as a public or private entity of a type referred to in the Annex, which has been identified as such by the Member State in accordance with Article 5 of the proposed RCE Directive. The explanatory part of the Proposal of the RCE Directive establishes ten sectors as a scope to the RCE Directive, and space is one of them.[135] The currently in force ECI Directive of which the proposed RCE will replace only applies to the energy and transportation sector.[136] Including space among several other sectors is a significant expansion in recognizing critical entities and infrastructure in the EU. The Proposal of the RCE Directive is meant to address the cross-border nature of more interconnected critical infrastructure networks and complement the proposed NIS 2 Directive.[137]

Article 14 of the proposed RCE Directive describes critical entities of particular European significance and establishes the need for specific oversight for these entities. The second subsection of Article 14 defines an entity as a critical entity of particular European significance if two conditions apply. Firstly, the entity has been identified as a critical entity, and it provides services for more than one-third of Member States, or the entity provides essential services. The Article further requires the Commission to be notified of the identification of the critical entity of particular European significance, and the Commission shall be responsible for informing the entity in question.[138]

[133] European Commission (EC), *supra nota*, 15, 9. (NIS2)
[134] European Commission (EC), *supra nota*, 16, 22. (RCE)
[135] *Ibid.*, 3. (RCE)
[136] *Ibid.*, 3.
[137] *Ibid.*, 1.
[138] *Ibid.*, 31.

IV. Critical space entities of the EU

The relevance of the space sector stems from the data and services it is capable of providing. The satellite data can be divided into scientific and research data, data used by governments and public authorities, commercial data for business to business or for consumer applications. The accuracy and security requirement and the acceptable margins for errors vary based on the types of satellite data used for an application.[139] A farmer relying on accurate meteorological and Earth observation data for its precision farming requires a higher degree of reliability from the data than the same farmer watching television using a satellite dish. A military unit performing a search and rescue mission error tolerance on navigation signal is significantly lower than for a tourist seeking out a bakery in Paris. Nevertheless, in all of the examples above, applications based on satellite data are used.

The farmer that operates in the EU and uses satellite data for precision farming expects the data he receives to be as accurate and precise as possible. Otherwise, building on a profitable business model would become difficult, and the benefits precision farming would provide become mute. Similarly, a military unit conducting a military training session on the Gulf of Finland relies on the accuracy of the navigation data and the security of the communication for its operation. In these examples, the military and the farmer are clients to the satellite data, and their willingness to use and rely on the provided data dictates the level of reliability of said data.[140] To increase the reliability of provided satellite data by the EU companies and within the EU, the cybersecurity requirements for these infrastructures need to respond to the clients' security needs.

The EU flagship programs Galileo, EGNOS, and Copernicus, provide a continuous stream of data to be used. The GPS and GNSS systems are used daily by people navigating cities using Google maps services, ships on route as maritime transportation, air traffic, autonomous drones, and many more. Interruptions in the navigation satellite operations can cause

[139] Jin, Z., Azzari, G. and Lobell, D.B., 2017. Improving the accuracy of satellite-based high-resolution yield estimation: A test of multiple scalable approaches. *Agricultural and forest meteorology*, *247*, pp.207-220, 207.
[140] Mazurelle, F., Wouters, J. and Thiebaut, W., 2009. The evolution of European space governance: policy, legal and institutional implications. *Int'l Org. L. Rev.*, *6*, p.155, 177.

significant disruption to daily lives. Navigation satellites, despite their high volume and high orbits, are not invulnerable to cyber threats.[141]

IV.I. Case study of EGNOS and Galileo

A large-scale denial of service incident happened in 2003 when a medium-size solar storm caused significant interference with the GPS satellites and derailed airplanes mid-flight.[142] Even though the 2003 incident was not man-made, the derailment of flights mid-air illustrates the dependence of navigation satellites as part of critical infrastructure.

Satellite navigation is vital for a wide range of terrestrial applications, from transportation to military operations. The Global Navigation Satellite Service (GNSS) is what provides global navigation. It is made up of the Chinese BeiDou Satellite System (BDS), European Galileo, Russian GLONASS, Indian Regional Navigation System (IRNSS)/Navigation Indian Constellation (NavIC), Japans Quazi-Zenith Satellite System (QZSS), and the United States Global Positioning System (GPS).[143] The six satellite navigation systems are subjects to different jurisdictions with different requirements for cybersecurity and data protection. The European Galileo system is regulated by the security measures outlined in the EU Space Program and the proposed NIS 2 Directive as per Article 2 (1) and (2). The Galileo space system falls under several requirements stated in the Article 2 (2) as the disruption of Galileo services would have a significant effect on public safety, security, and health (d), the disruption would have a cross-border effect (e), and it has specific importance at regional and national levels for particular sector and type of services (f).

[141] Schmidt, D., Radke, K., Camtepe, S., Foo, E. and Ren, M., 2016. A survey and analysis of the GNSS spoofing threat and countermeasures. *ACM Computing Surveys (CSUR)*, *48*(4), pp.1-31.

[142] *Halloween Storms of 2003 Still the Scariest.* NASA. Retrieved from https://www.nasa.gov/topics/solarsystem/features/halloween_storms.html, March 14, 2

[143] *Other Global Navigation Satellite Systems (GNSS).* GPS. Retrieved from https://www.gps.gov/systems/gnss/, March 20, 2021.

Galileo is an independent European satellite navigation system that provides global positioning. Galileo was developed with funding from the European Commission.[144] Galileo is part of GNSS and provides geo-positioning signals for many applications and clients within the European and surrounding regions. An accurate geo-positioning signal is calculated based on three to four parameters, each supplied by a separate navigation satellite on different orbital positions.[145] Figure 1 shows the principles of satellite-based positioning. The satellite's geometric distance to the receiver is measured by the run time[146] it takes for a signal to reach the receiver from the satellite.[147] The navigation satellite system is built upon specialized satellite clocks that measure the time as accurately and synchronously as possible.[148] Galileo's satellite system uses high-accuracy clocks, which calculates the time it takes for a satellite signal to reach the receiver using the speed of light as a constant. High accuracy atomic clocks use the stable frequency of the radiation of the atom when it jumps from one energetic state to another to calculate the passing of time.[149] The relevance of the timing stems from the triangulation principle, as mentioned above. For a single geo-location to be determined, three satellites are must measure different values needed to calculate the accurate position. The accurate time measurement and a speed constant make the triangulation result relatively accurate.

[144] GSA, *supra nota,* 29.

[145] Hofmann-Wellenhof, B., Lichtenegger, H. and Wasle, E., 2007. *GNSS–global navigation satellite systems: GPS, GLONASS, Galileo, and more*. Springer Science & Business Media, 3.

[146] Indicated with a `T` on Figure 1.

[147] Hofmann-Wellenhof, Lichtenegger, and Wasle, (2007), *supra nota*, 145, 3.

[148] Senior, K.L., Ray, J.R. and Beard, R.L., 2008. Characterization of periodic variations in the GPS satellite clocks. *GPS solutions, 12*(3), pp.211-225, 212.

[149] *Galileo's Clock.* ESA. Retrieved from https://www.esa.int/Applications/Navigation/Galileo/Galileo_s_clocks, March 19, 2021.

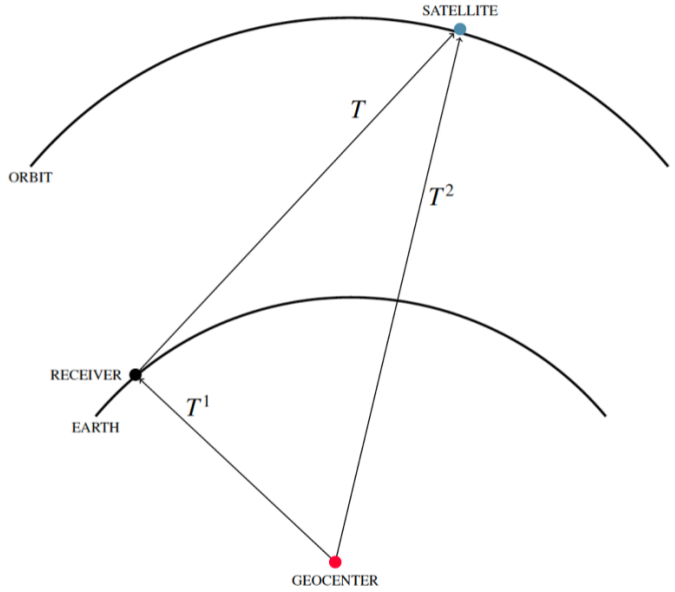

Figure 1. Principle of satellite-based signal, where T indicates the time it takes for signal to travel from one point to another.
Source: Hofmann-Wellenhof, B., Lichtenegger, H. and Wasle, E., 2007. *GNSS–global navigation satellite systems: GPS, GLONASS, Galileo, and more*. Springer Science & Business Media, 4.

Navigation satellites are vulnerable to jamming and spoofing attacks on the satellite signal for triangulation resulting in errors to the receiver. Encryption mechanisms on the GNSS systems are designed to mitigate spoofing attacks.[150] The Galileo system has five levels of encryptions based on the purpose of the application.[151] The open and unrestricted access is based on the same principle as the GPS signal's release to the public.[152] The purpose of the unrestricted access for the general use of the public is to enable the development of services and serve general interests.[153] The most critical applications of the Galileo systems are the Safety of Life Services and Search and Rescue, which require absolute reliability, quality, and therefore have

[150] *GNSS Authentication and encryption.* ESA Navipedia. Retrieved from https://gssc.esa.int/navipedia/index.php/GNSS_Authentication_and_encryption, April 2, 2021.

[151] European Commission Directorate-General for Transport and Energy, *Midterm Evaluation of the Galileo project for the period 2002-2004. Final Report*, June 2006, 4.

[152] *Why the Military released GPS to the Public*. Popular Mechanics. Retrieved from https://www.popularmechanics.com/technology/gadgets/a26980/why-the-military-released-gps-to-the-public/, April 4, 2021.

[153] European Commission Directorate-General for Transport and Energy, (2006), *supra nota*, 151, 4.

the highest encryption levels.[154] The Safety of Life and Research and Rescue services are high-impact services for any cyber intrusion making the Galileo system a critical entity of particular European significance per Article 14 of the proposed RCE Directive. Galileo additionally caters to the European public authorities for civil protection, national security, and law enforcement needs. The bandwidth used on these services has anti-jamming and anti-spoofing encryptions that should withstand malicious interference.[155] Galileo provides a wide range of services for consumer, commercial and critical infrastructure. Different services provided by Galileo can fall either under the proposed NIS 2 Directive or RCE Directive. Whether the proposed NIS 2 Directive of the RCE Directive applies should be made based on the specific service and its potential impact.

Galileo, however, is not the only navigational space system by the EU. The EGNOS is a regional satellite-based augmentation system to improve the GNSS performance in Europe.[156] EGNOS is needed to improve the GNSS signal that otherwise could have an error range up to five meters.[157] Minimizing error range is specifically necessary for critical applications such as providing support for transportation. Figure 2 illustrates how the EGNOS system supports the GNSS system of which Galileo is part. The EGNOS consists of four parts that all support each other.

The space element consists of three geostationary (GEO) satellites.[158] The use of three GEO satellites stems from the triangulation principle needed to determine the receiver's accurate position, as is illustrated in Figure 1. The EGNOS satellites are sufficient in independently providing the three necessary inputs needed for determining geo-position – latitude, longitude, and height.[159] Nevertheless, the EGNOS is built to receive and augment signals from any of the six GNSS systems.

[154] European Commission Directorate-General for Transport and Energy, (2006), *supra nota,* 151, 4

[155] *Ibid.*

[156] GSA, *supra nota,* 29.

[157] Wu, W., Guo, F. and Zheng, J., 2020. Analysis of Galileo signal-in-space range error and positioning performance during 2015–2018. *Satellite Navigation*, *1*(1), p.6., 6.

[158] Wu, W., Guo, F. and Zheng, J., (2020), *supra nota*, 157, 6; GEO is an orbit located at 35 700 km above the Earth's equator and what makes GEO unique is the time it takes for the satellite to make a full orbit is the same as Earth's rotation. Therefore, the satellite on GEO appears to be positioned stationary at one point in the sky.

[159] Hofmann-Wellenhof, Lichtenegger, and Wasle, (2007), *supra nota,* 113, 3.

The EGNOS receiving ground stations receive the signal from the GNSS satellites, then direct it to one of the processing centers, which directs the augmented signal to the ground station that sends the signal to the EGNOS satellites. In the example in Figure 2, the red dot illustrates an airplane in flight as the final user, which uses the signals from the GNSS 2 satellite and the augmented signals from two EGNOs satellites.

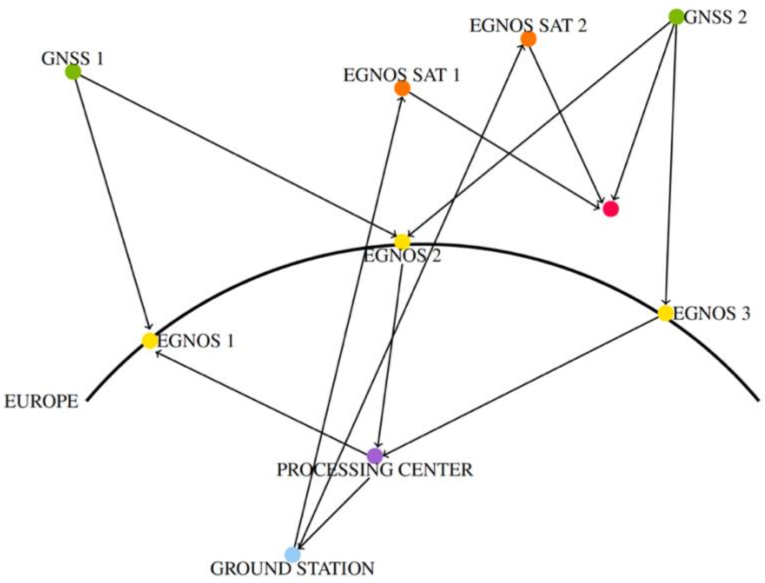

Figure 2. How the EGNOS system works: Author´s visualization based on information provided by Morton, Y.J., van Diggelen, F., Spilker Jr, J.J., Parkinson, B.W., Lo, S. and Gao, G. eds., 2020. *Position, Navigation, and Timing Technologies in the 21st Century, Volumes 1 and 2: Integrated Satellite Navigation, Sensor Systems, and Civil Applications, Set*. John Wiley & Sons, and the European Space Agency.

As shown in Figure 2, the EGNOS has a network of different ground-based elements for receiving, broadcasting, and processing the signal. The ground-based systems are divided into 40 ranging integrity monitoring stations (RIMS), two mission control centers (MCC), six navigation land earth stations (NLES), and EGNOS wide area network (EWAN).[160] The RIMS are located in a parse area across the European region. RIMS are indicated as EGNOS 1,2,3 in Figure 2 and collect the navigation data from the GNSS satellites and transmit the data to the

[160] *EGNOS System.* GSA. Retrieved from https://www.gsa.europa.eu/european-gnss/egnos/egnos-system, April 6, 2021.

central processing facilities located with the MCC, indicated as processing center in Figure 2. The task of the MCC is to collect the data and correct any errors within the received data. The corrected data is then sent to the NLES or the ground station in Figure 2, which in turn transmits the corrected navigation signal data to the EGNOS satellites on GEO. For redundancy purposes, two NLES ground stations service each EGNOS satellite.[161] The EGNOS system implements many principles associated with the cybersecurity-by-design recommended for the use of secure air traffic by the Tallinn Manual 2.0.[162]

The cybersecurity-by-design principle is guided by the goal to reduce the attack surfaces of any given moment based on the system's design and therefore provide high resilience to the system.[163] The system design that provides security over EGNOS is its 40 RIMS which collects data from GNSS satellites overhead in any given second. The main cybersecurity threat to satellite navigation systems is spoofing.[164] As explained above, spoofing creates a faulty signal through signal manipulation. There are different ways to create a false navigation signal.[165] The security by design used for the building of EGNOS allows the system to be more resilient to these spoofing attacks taking into account the technical aspects of spoofing.

The ground station is the part of the space system that receives communication from the satellite and can send operational or other signals back to the satellite. One attack vector presented this way for GNSS signals is creating a false *ad hoc* ground station pretending to send augmented signals to the navigation satellite.[166] The security-by-design solution that helps detect and counter such attacks on the EGNOS satellites is the NLES and the requirement for a single EGNOS satellite to be serviced by two NLES at any given time.[167] In order to transmit a corrupted navigational signal to the EGNOS satellite in orbit, both NLES ground segments servicing the same EGNOS satellite on GEO should be spoofed at the same time. However, the NLES ground stations are not located in the same place but are distributed across the area

[161] GSA, *supra nota*, 160.
[162] Schmitt, M.N. ed., 2017. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press, 269.
[163] *Cybersecurity by design: building in the protection from the ground up.* Thales. Retrieved from https://www.thalesgroup.com/en/market-specific/critical-information-systems-and-cybersecurity/magazine/cybersecurity-design, April 6, 2021.
[164] Falco, (2018), *supra nota*, 2, 6.
[165] *Ibid.*
[166] Falco, (2018), *supra nota*, 2, 6.
[167] GSA, *supra nota*, 160.

of the EU.[168] For the successful transmission of the falsified signal, the *ad hoc* ground stations would need to intersect and replace both NLES ground stations synchronously.

Another method of attacking a navigational signal is compromising a receiver and altering the output signal of the satellite.[169] For EGNOS, that would mean compromising any of the 40 RIMS distributed across the EU. The RIMS are EGNOS receiving ground stations, but the RIMS do not create positioning outputs on their own, rather, the task of the RIMS is to collect navigation data and forward it to MCC-s for correction. The underlying principle for the RIMS process is that the received input data can be corrupted and by continuously collecting data from all GNSS satellites overhead and matching them to other RIMS collections, the inherent error in the signal will be corrected.[170] Hence, corrupting the RIMS receiver data is futile as the RIMS system is designed to counter errors in the received navigational signal. The system of RIMS and NLES effectively implements the principles of security-by-design and significantly reduce attack surface area for the EGNOS while simultaneously counter malicious corruptions already present.

This, however, does not mean that the EGNOS and Galileo systems are invulnerable to cyber-attacks. The ex-post evaluation conducted on the activities of the GSA and the governance of both EGNOS and Galileo exposed several inefficiencies and areas of improvement on the security governance of Galileo and EGNOS.[171] Based on Anderson's definition, to create resilience in the entirety of the system, all levels of the system have to be considered.[172] The definition for the system that Anderson provided included internal users, management, and the IT staff.[173] The opinion of many cybersecurity scholars is that the human element is the cause of the majority of attack vulnerabilities. Anderson describes the tendency to choose visible cybersecurity policies over effective ones because they tend to create a feeling of safety and provide political favor to the decision-maker and refers to this phenomenon as `Security Theatre`.[174] Similarly, one of the most effective initial entries to a system is done through phishing, requiring an individual within the system to fall prey to a phishing attack.[175] A

[168] GSA, *supra nota,* 160.
[169] Falco, (2018), *supra nota,* 2, 6.
[170] GSA, *supra nota,* 160.
[171] Commission Proposal (EC), *supra nota*, 8, 6. (Space Program)
[172] Anderson, (2020), *supra nota,* 84, 12.
[173] Anderson, (2020), *supra nota,* 84, 12.
[174] *Ibid.*, 7.
[175] Usenix, *supra nota,* 78.

behavior described by NSA Director of Cybersecurity, Rob Joyce, that falls under the security theatre category is the conduction of red team testing on systems but failure to follow through with fixing the vulnerabilities indicated in the reports.[176] This thesis is not trying to suggest that the previously mentioned human vulnerabilities are present in the EU EGNOS and Galileo systems. These vulnerabilities are mentioned to draw attention that if the technical system itself can be designed to be resilient such as EGNOS and Galileo are, the attack surface that remains stands with people who work, manage and operate in or around the systems. Furthermore, as indicated with the ex-post evaluation of EGNOS and Galileo, the vulnerability of human elements was detected in the security governance. It is to be seen whether the indicated vulnerabilities will be addressed or EGNOS and Galileo fall into the trap of `security theatre`.

IV.II. Case study of Copernicus

The EU's second flagship space program is the earth observation (EO) system Copernicus.[177] The Copernicus system consists of space elements and *in situ* sensors.[178] The purpose of the Copernicus program is to gather relevant data on Earth. Copernicus space element is divided into different types of satellites based on the data they collect. The Copernicus EO satellites are named Sentinel and are assigned a number to indicate the type of EO data gathered.[179] This distinction is necessary as the cameras and sensors onboard require different technical capabilities for capturing information on different wavelengths.[180]

Sentinel-1 satellites carry radar technologies for providing day and night weather information.[181] Sentinel-1 data provides data for a myriad of applications allowing for the monitoring of climate change, mapping crops, measuring forests biomass, floods, traffic jams, shorelines, to name a few.[182] Sentinel-2 are satellites that carry high-resolution multispectral imagers with 13 spectral bands available for land and vegetation observance.[183] High-

[176] Usenix, *supra nota*, 78

[177] Reillon, V., (2017), *supra nota*, 23, 1.

[178] *Infrastructure overview*. Copernicus. Retrieved from https://www.copernicus.eu/en/about-copernicus/infrastructure-overview, April 6, 2021.

[179] *Ibid.*

[180] Joseph, G., 2015. *Building earth observation cameras*. CRC press, 75.

[181] *Sentinel – 1*. ESA. Retrieved from http://www.esa.int/Applications/Observing_the_Earth/Copernicus/Sentinel-1, April 6, 2021.

[182] *Ibid.*

[183] *Sentinel – 2*. ESA. Retrieved from http://www.esa.int/Applications/Observing_the_Earth/Copernicus/Sentinel-2, April 6, 2021.

resolution multispectral satellite data have a wide range of applications for sectors with links to critical services such as precision farming[184] or tracking of infectious diseases.[185] Furthermore, Sentinel 1 satellites are capable of providing near-real-time (NRT) data for emergency response in maritime situational awareness and security,[186] and wildfire monitoring and response[187]

Sentinel – 3 is designed for sea and land surface temperature measurements, ocean, and land surface color measurements and has high accuracy for ocean forecasting, environmental and climate monitoring.[188] The Sentinel-3 hosts an onboard radiometer for sea and land surface temperature, synthetic aperture radar (SAR) altimeter, microwave radiometer, instruments for precise orbit determination, and instruments for measuring land and ocean color.[189] The Sentinel-3 hosts a wide range of different payloads that collect and combine measurements for a diverse catalog of applications.

Sentinel – 4 and Sentinel -5 missions are to monitor air and atmospheric quality over Europe at high spatial resolution and fast revisit time.[190] Sentinel -5 supports Sentinel -4 with gathering ozone and surface UV measurements. The Sentinel – 5 hosts a high-resolution spectrometer operating on the shortwave infrared range.[191] In addition to the different types of satellites, the Copernicus system also has several terrestrial segments composed of third parties' elements.[192]

The type of comprehensive security-by-design approach present in the EGNOS system is not present in the Copernicus system. EGNOS system is a single comprehensive system designed

[184] Gevaert, C.M., Suomalainen, J., Tang, J. and Kooistra, L., 2015. Generation of spectral–temporal response surfaces by combining multispectral satellite and hyperspectral UAV imagery for precision agriculture applications. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, *8*(6), pp.3140-3146, 3140.

[185] Roberts, D.R., Paris, J.F., Manguin, S., Harbach, R.E., Woodruff, R., Rejmankova, E., Polanco, J., Wullschleger, B. and Legters, L.J., 1996. Predictions of malaria vector distribution in Belize based on multispectral satellite data. *The American journal of tropical medicine and hygiene*, *54*(3), pp.304-308, 3

[186] Krause, D., Schwarz, E., Voinov, S., Damerow, H. and Tomecki, D., 2019. Sentinel-1 near real-time application for maritime situational awareness. *CEAS Space Journal*, *11*(1), pp.45-53, 45.

[187] Ban, Y., Zhang, P., Nascetti, A., Bevington, A.R. and Wulder, M.A., 2020. Near real-time wildfire progression monitoring with Sentinel-1 SAR time series and deep learning. *Scientific reports*, *10*(1), pp.1-15, 1.

[188] *Sentinel – 3.* ESA. Retrieved from https://sentinel.esa.int/web/sentinel/missions/sentinel-3, April 6, 2021.

[189] ESA, *supra nota*, 154.

[190] *Sentinel – 4.* European Space Agency. Retrieved from https://sentinel.esa.int/web/sentinel/missions/sentinel-4, April 6, 2021.

[191] *Sentinel – 5.* European Space Agency. Retrieved from https://sentinel.esa.int/web/sentinel/missions/sentinel-5, April 6, 2021.

[192] *Collaborative Ground Segment.* European Space Agency. Retrieved from https://sentinel.esa.int/web/sentinel/missions/collaborative, April 9, 2021.

to execute a single task to perfection, and the purpose of the task creates a design that reduces the attack surface for the system. The Copernicus, on the other hand, is a program that consists of many different nodes providing different types of data without a central core task. Copernicus is designed to collect and synthesize data that is relevant for different terrestrial applications. The Copernicus data can be downloaded by several ground stations located in all the regions of the EU.[193] Without the centralized MCC from where all relevant data flows through, the attack vectors for the Copernicus systems are singular in the sense that each satellite and ground station work in seclusion and a coordinated attack that would cascade across the entire Copernicus system is difficult, if not impossible, to execute. The attack vector with the most concern for the Copernicus system is the supply chain due to the high complexity and diversity of instruments used on its Sentinel satellites, as was illustrated above.

The Space Strategy for Europe brings out the need to address the vulnerable position of the European space industry in its second priority due to its high dependence on global supply chains and non-European origin of critical components and technologies.[194] The EDA list for the European non-dependence in the space sector contains 48 different technologies required for building and developing different subsystems of satellites.[195] Technologies directly relating to the cybersecurity of the Sentinel satellites are high speed digital to analog converter and analog to digital converter for EO data distribution;[196] European availability, access, and compatibility of publicly-funded IP Cores for space;[197] the development and qualifications of programmable read-only memory (PROM);[198] development of controller area network (CAN) bus compliant with ISO requirements for growth in reliance, unrestricted access, and data integrity;[199] development of high-performance data compression algorithms to cope with the large data sets generated by satellites.[200] Some of the items listed below are under the International Traffic in Arms Regulation (ITAR) export restrictions. However, the items highlighted bear a significance in ensuring higher cybersecurity on European space assets as supply chain vulnerabilities are one of the most exploited attack vectors for space systems.[201]

[193] *Collaboration Categories.* European Space Agency. Retrieved from https://sentinel.esa.int/web/sentinel/missions/collaborative/categories, April 9, 2021.

[194] European Commission (EC), *supra nota*, 31, 5. (space strategy)

[195] EC, ESA, EDA, (2015), *supra nota*, 109.

[196] *Ibid.*, 21.

[197] *Ibid..*, 40.

[198] *Ibid.*, 44.

[199] *Ibid.*, 45.

[200] *Ibid.*, 50.

[201] Falco, (2018), *supra nota*, 2, 3.

The proposal for NIS 2 Directive Article 19 addresses the vulnerabilities of ICT critical supply chains and the need to assess the risk factors associated with them. Article 11 of the proposal for the RCE Directive obliges the Member States as part of building resilience to identify alternative supply chains for critical entities. Including space as an element of critical infrastructure with the proposals for NIS 2 and RCE gives the Member States and the EU ability to implement stricter regulations in ensuring the security of supply chains for space components as well as to allocate funds for research and development activities in the EDA identified critical components for space. The Copernicus system is more difficult to allocate to a single proposed Directive. The Copernicus, as mentioned above, has several different purposes. Not all Sentinel satellites cater to critical or essential services or infrastructures. Sentinel 1 and its maritime situational awareness and security and wildfire monitoring services, however, do fall under critical entities requirement per Article 2 (2) of the proposed NIS 2 Directive.

IV.III. Case study of mega-constellations and CubeSats

Since the 2000-s, there has been an explosion in the development of space-based services provided by several private start-ups operating satellites for EO and, more recently, in communication.[202] This phenomenon is called NewSpace, and as mentioned above, it is a start-up-like ecosystem for merging space companies. The technical innovation that helped the emergence of NewSpace was the creation of the CubeSat standard. The California Polytechnic State University developed CubeSat standard in 1999 to help university students develop satellites for educational purposes to launch to low earth orbit (LEO).[203] What made CubeSats such a revolutionary innovation was its size, technological capabilities, and universal applicability. CubeSats are measured in units (U) in where one unit equals 10x10x11 cm.[204] The universal applicability that the CubeSats made possible was the development of CubeSat dispenser systems.[205] he development of CubeSat dispenser system meant that a launcher could use the vehicle room more efficiently when all satellites follow the same size standards and

[202] *Space Economy at a Glance*. OECD. Retrieved from http://www.oecd.org/sti/futures/space/48301203.pdf, March 15, 2021.

[203] *The CubeSat Program*. CubeSat. Retrieved from https://www.cubesat.org/about/, March 20, 2021.

[204] *CubeSat 101. Basic Concepts and Processes for First-Time CubeSat Developers*. NASA. Retrieved from https://www.nasa.gov/sites/default/files/atoms/files/nasa_csli_cubesat_101_508.pdf, March 20, 2021.

[205] *Ibid.*

can be similarly attached to the launch vehicle, hence make it possible to maximize the available room to a maximum number of satellites being launched at a time.[206] This development, in turn, reduced the launch price for a single functioning satellite and the standardization of the CubeSats gave rise to the production of commercial off-the-shelf components (COTS).[207] Companies started to mass-produce solutions for different satellite subsystems to predict will fit into the CubeSat standard.[208]

The wide use of COTS components has helped the emergence of companies capable of reducing development and costs and to speeding up the development to launch time. In addition, the higher performance per unit allows the companies to take full advantage of lower launch costs that are available due to the developed CubeSat dispenser system.[209] These developments have allowed the NewSpace companies to implement rapid development cycles while reducing costs, allowing for more frequent satellite launches.

These advancements in technology caused the EO sector of the space industry to increase in its economic value, with several global private companies emerging that build their business plans on the different EO capabilities, many of them similar to Sentinel satellites.[210] The centralization and systems design can be different for private companies providing EO data. The EU Copernicus program is built on the principle of free availability of data.[211] Private companies tend to be less open with their data distribution and create ready-made products to sell to their clients. These products involve creating predictive algorithms that run on the EO data they collect from their private satellite constellations.[212] The private EO companies provide services to a large array of industries, including the public administration and defense industry.[213] The business side of the EO has led to the emergence of companies that build and launch large satellite constellations and mega-constellations globally and in Europe. Two

[206] NASA, *supra nota,* 204.
[207] OECD, *supra nota,* 202.
[208] *Ibid.*
[209] *Ibid.*
[210] *The Top 10 Hottest Satellite Companies in 2020.* ViaSatellite. Retrieved from http://interactive.satellitetoday.com/via/march-2020/the-top-10-hottest-satellite-companies-in-2020/, April 9, 2021.
[211] *Use Typologies and Available Services.* European Space Agency. Retrieved from https://sentinel.esa.int/web/sentinel/sentinel-data-access/typologies-and-services, April 9, 2021.
[212] *Maritime data with unrivalled ocean coverage.* Spire. Retrieved from https://spire.com/maritime/, April 9, 2021.
[213] *Federal data solutions.* Spire. Retrieved from https://spire.com/federal/, April 11, 2021; *Actionable Satellite data for industry use cases from Iceye,* ICEYE, Retrieved from https://www.iceye.com/use-cases, April 11, 2021.

significant emerged companies operating within Europe that operate satellite constellations for EO are ICEYE from Finland and Spire that has offices in Europe, United States, and Asia.

Article 2 of the NIS 2 Directive proposal defines its scope to include the private companies, and its subsection 2 gives exemptions to include companies regardless of their size as subjects to the NIS 2.[214] The proposal for RCE Directive defines a critical entity as an entity providing one or more essential services. An incident would have significant disruptive effects on the provision of the services or other essential services in the sectors identified as critical.[215]

The Finnish company ICEYE provides services to the financial, energy, and security sectors.[216] Spire, similarly, caters to the same profile of customers.[217] According to the proposals of NIS 2 and RCE Directives, energy, security, and financial sectors fall under the sectoral scopes of both directives making ICEEYE and Spire potential subjects to these Directives as critical entities. The proposals for NIS 2 and RCE have different approaches to how critical entities are identified. The proposed RCE Directive grants the discretion to decide whether an entity is a critical infrastructure to the Member States to decide per Article 5. However, the proposed NIS 2 Directive does not address a specific form of action for Member States in implementing rules over elements described in Article 2. It does, however, instruct the drafting and adopting of national cybersecurity strategies in implementing strategic objectives and appropriate policy and regulation measures to achieve and maintain a high level of cybersecurity.[218]

Article 5 of the proposed NIS 2 Directive lays out obligations of Member States in creating national cybersecurity strategies, and in its subsection 2 (h) it states that the Member States shall adopt a policy addressing specific needs of SMEs, in particular those excluded from the scope of this Directive, to provide guidance and support in their resilience to cybersecurity threats.[219] The wording of subsection 2 (h) of Article 5 implies that any SME or company that falls under the defined scope of Article 2 is subject to the Member States cybersecurity strategy and policy measures stated in the proposed NIS 2 Directive.

[214] European Commission (EC), *supra nota*, 15, 30. (NIS2)

[215] European Commission (EC), *supra nota*, 16, 25. (RCE)

[216] ICEYE, *supra nota*, 174.

[217] *Maritime data with unrivalled ocean coverage.* Spire. Retrieved from https://spire.com/maritime/, April 9, 2021.

[218] European Commission (EC), *supra nota*, 15, 34. (NIS2)

[219] *Ibid., 35*. (NIS2)

Cyber-attacks on space assets are rare, but they do occur. The nature of these attacks is generally motivated by gaining geopolitical influence or providing national defense.[220] The vulnerabilities of European critical infrastructure that interconnects with the space element are necessary to protect, and what we see in the proposals for NIS 2 Directive and the RCE Directives is derived from potential security and defense considerations. Cyber intrusions, however, can fall under three distinctive categories – hacktivism, nation-states hackers, and criminal activity.[221] Cyber intrusions on space tend to fall under two of these categories – hacktivism and adversarial nation-states attempting to gain the geopolitical advantage.[222]

The emergence of centralized satellite constellations on LEO with lower requirements for cybersecurity creates perfect conditions for a satellite-to-satellite attack using compromised satellites in targeting other satellites in orbit. [223] What makes satellites developed and deployed by commercial entities even more vulnerable is the widespread use of commercial off-the-shelf (COTS) components.[224]

Regardless of the type of the satellite, all satellites have similar basic subsystems, which are mechanical structure (satellite bus), propulsion, thermal control, power supply, telemetry, tracking and control (TT&C), altitude and orbit control (AOCS), payload, and communication.[225] Each of the named subsystems consists of several other systems within themselves. Based on the satellite being manufactured, different approaches can be made in building, designing, and manufacturing these subsystems.[226] For fast development cycle, satellite operators use COTS components. COTS components can range from full satellites and satellite subsystems to more minor elements used in a satellite building. COTS components can mean that different producers make the different parts of the satellite, and the primary satellite operator compiles the final satellite.[227] It can similarly mean that the entire satellite is in itself a COTS and is bought ready to launch. [228]

[220] Unal, (2019), *supra nota*, 7,6.
[221] Blount, P.J, (2017), *supra nota*, 1, 279.
[222] *The Cyber Threat to Satellites*, The Strategist, Retrieved from https://www.aspistrategist.org.au/the-cyber-threat-to-satellites/, May 3, 2021.
[223] Falco, G., (2020), *supra nota*, 97, 2.
[224] Falco, G., (2018), *supra nota*, 2, 4.
[225] Maini, A.K. and Agrawal, V., 2011. *Satellite technology: principles and applications*. John Wiley & Sons, *4.1*.
[226] *Ibid.*
[227] Falco, (2018), *supra nota*, 2, 3.
[228] *Ibid.*, 3.; *Boeing Satellites*. Boeing. Retrieved from https://www.boeing.com/space/boeing-satellite-family/, March 15, 2021.

The availability of COTS components implies that anyone with financial means to purchase a COTS element can access them, analyze them and identify exploitable vulnerabilities.[229] Additional vulnerability with COTS stems from the fact that COTS components rely on software updates provided by their manufacturer. If a satellite operator determines a mistake or a vulnerability in the COTS software, they depend on the COTS producer to provide the necessary update at a necessary timeframe.[230] Reliance on the COTS manufacturer for software updates can create a myriad of complications. Delayed fixes, bugs in software codes, or unwillingness to provide an update or a fix at all.[231] As a result of widespread unreliable software fixes provided by the manufacturer, in 2019, the European Union adopted a Directive on the sale of goods to include the sale of digital goods and the requirement for software maintenance.[232]

Another vulnerability that stems from the use of COTS components is the accessibility dictated by the complexities of the supply chain of different elements.[233] The challenges with the supply chain were addressed in more detail earlier while discussing the European technological non-dependence within the space sector.

The proposal for the NIS 2 Directive addresses the vulnerabilities of the European supply chain and the need to increase the security of it through different measures and proposes an EU coordinated risk assessment for critical supply chains.[234] The proposal for the RCE Directive Article 11 (1) (d) obliges to identify alternative supply chains as a vital measure in providing resilience of critical entities. Challenges stemming from the supply chain are not unique to the private sector operating satellites. As mentioned earlier, the EDA has identified 48 technological priorities for EU non-dependence in the space sector, which are all exclusively technological and predominantly provided by entities outside of the EU.[235] What makes the private sector different from the EU flagship space programs Galileo, EGNOS, and Copernicus is that the EU flagship programs are subject to the supervision of the SAB. The private sector,

[229] Usenix, *supra nota,* 78.
[230] Falco, G., (2018), *supra nota*, 2, 5.
[231] Falco, G., (2018), *supra nota*, 2, 5.
[232] Directive (EU) 2019/771/EC on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, OJ L 136/28, 22.5.2019.
[233] Falco, G., (2018), *supra nota*, 2, 4.
[234] European Commission (EC), *supra nota*, 15, 46. (NIS2)
[235] EC, ESA, EDA, (2015), *supra nota,* 109.

however, tends to make decision based on cost estimates and profitability. Therefore, unless the law does not impose security requirements, companies might not opt to make higher expenditures in favor of security.

Expanding the scope of the proposed NIS 2 and RCE Directives to include private and public space entities in various sizes and posing additional cybersecurity requirements and national oversight allows for the emergence of relevant technological research and development within the EU. The EU Space Program and its flagship systems have always had higher standards than the private sector that makes its decision based on profit margins and is tempted to cut costs. The proposed NIS 2 and RCE Directives would implement requirements for companies to invest in components with certified security. The proposed NIS 2 and RCE Directive, in collaboration with identified key technologies for the European non-dependence by the EDA, has the potential in facilitating the growth of the cybersecurity market for space within the EU. If the Member States will not oppose including space in the proposed NIS 2 and RCE Directives stating the TFEU Article 189 and the prohibition of the EU-wide harmonizing legislation regarding space.

V. Conclusion

This thesis posed two research questions: (1) how much of the EU space systems and space industries fall under the scopes of proposed NIS 2 and RCE Directives and (2) to analyze the effect of legal requirements for security-by-design and resilience policies on EU space system.

The proposals for the NIS 2 and the RCE Directives include space within its defined scope of sectors. The inclusion of space as a sectoral scope comes regardless of the restrictions stated in the TFEU to prevent the EU from adopting EU-wide harmonizing legislation on space programs. The TFEU establishes parallel competency in the area of space programs. The TFEU, however, addresses the harmonization of space programs but not space as it would relate to other sectors and industries. The proposals for NIS 2 and RCE Directives approach space through interoperability with other sectors as the space element extends into critical infrastructure.

The Space Strategy for Europe adopted in 2016 establishes four distinct priorities for developing the space sector within the EU. Each of these highlights the interoperability and the convergence of technologies and sectors. The Union Space Program agreed among the Member States incorporates five flagship programs (EGNOS, Galileo, Copernicus, SST, GOVSATCOM) under single governance. From the different regulations, a broad framework for European space systems can be drawn. Broadly, there are four areas of space within the EU with different legal standing. The national space programs exempt from EU-wide harmonizing regulation and space systems that are indistinguishably converged with critical infrastructure and fall under the proposed NIS 2 and RCE Directives. The EU space program, that consists of its five flagship programs, and private NewSpace companies whose activities do not meet the requirements set out in the NIS 2 and RCE Directives to fall under its scope.

Many NewSpace companies do not meet the requirements set out in Article 2 (2) of the proposed NIS 2 Directive or Article 1 of the proposed RCE Directive. The applicability of the proposed NIS 2 and RCE Directives are similarly not homogeneous across the five EU flagship space programs. EGNOS and Galileo are singular systems with a single purpose to provide satellite navigation signals and are easily identifiable as critical infrastructure. On the other hand, Copernicus is more complex with a multitude of purposes and technologies ranging from a wide area of applications. This results in each particular application and service the Copernicus system provides to be assessed independently as critical infrastructure per proposed NIS 2 and RCE Directives. The thesis did not address the SST, and GOVSATCOM programs as SST is related to traffic management in orbit and GOVSATCOM is not yet operational.

The aspect of the space system that could benefit the most from the proposed NIS 2 and RCE Directives is the security of the supply chain. The supply chain for space elements has been identified as one of the most vulnerable aspects. The EDA has addressed the European need for non-dependence within the space sector by compiling a list of technologies to be developed within the EU. The EU is currently dependent on third-country supplies on these technologies. The vulnerabilities posed by the supply chain are further complicated by the widespread use of COTS components and varying security requirements in the manufacture of COTS components. The supply chain aspect of cybersecurity for space systems and its security by design is the most vulnerable and will require significant funding for capacity building in the EU.

The legal landscape governing the space sector within the EU is complex, and determination on the applicability of the proposed NIS 2 and RCE Directives on any given system should be separately assessed. The TFEU grants the Member States an opportunity to oppose the inclusion of space in EU-wide harmonization legislation. Including space into the proposals for the NIS 2 and the RCE Directives would allow for more harmonious cybersecurity standards for different space systems within the EU and could help to make available tools for developing critical technologies for European non-dependence. The benefit for the EU and the Member States would be plentiful with higher security on critical entities with space element and by capacity building for critical technologies.

Bibliography

Scientific Books

1. Anderson, R., 2020. *Security engineering: a guide to building dependable distributed systems*. John Wiley & Sons.
2. Brenner, S.W., 2009. *Cyberthreats: The emerging fault lines of the nation state*. Oxford University Press.
3. Hofmann-Wellenhof, B., Lichtenegger, H. and Wasle, E., 2007. *GNSS–global navigation satellite systems: GPS, GLONASS, Galileo, and more*. Springer Science & Business Media.
4. Joseph, G., 2015. *Building earth observation cameras*. CRC press.
5. Lessig, L., 2009. *Code: And other laws of cyberspace*. ReadHowYouWant.com.
6. Maini, A.K. and Agrawal, V., 2011. *Satellite technology: principles and applications*. John Wiley & Sons.
7. Pellegrino, M. and Stang, G., 2016. *Space security for Europe*. EU Institute for Security Studies.
8. Schmitt, M.N. ed., 2017. *Tallinn manual 2.0 on the international law applicable to cyber operations*. Cambridge University Press.
9. von der Dunk, F. ed., 2015. *Handbook of space law*. Edward Elgar Publishing.

Academic Articles

10. Ban, Y., Zhang, P., Nascetti, A., Bevington, A.R. and Wulder, M.A., 2020. Near real-time wildfire progression monitoring with Sentinel-1 SAR time series and deep learning. *Scientific reports*, *10*(1), pp.1-15.
11. Benson, V., McAlaney, J. and Frumkin, L.A., 2019. Emerging threats for the human element and countermeasures in current cyber security landscape. In *Cyber Law, Privacy, and Security: Concepts, Methodologies, Tools, and Applications* (pp. 1264-1269). IGI Global.
12. Blount, P.J., 2017. Satellites are just things on the internet of things. *Air and Space Law*, *42*(3).
13. Cheng, B., 1983. The legal status of outer space and relevant issues: Delimitation of outer space and definition of peaceful use. *J. Space L.*, *11*, (p.89).
14. Falco, G., 2018. The vacuum of space cyber security. In *2018 AIAA SPACE and Astronautics Forum and Exposition* (p. 5275).

15. Falco, G., 2019. Cybersecurity principles for space systems. *Journal of Aerospace Information Systems*, *16*(2), pp.61-70.
16. Falco, G., 2020. When Satellites Attack: Satellite-to-Satellite Cyber Attack, Defense and Resilience. In *ASCEND 2020* (p. 4014).
17. Fritz, J., 2013. Satellite hacking: A guide for the perplexed. *Culture Mandala*, *10*(1), p.5906.
18. Gevaert, C.M., Suomalainen, J., Tang, J. and Kooistra, L., 2015. Generation of spectral–temporal response surfaces by combining multispectral satellite and hyperspectral UAV imagery for precision agriculture applications. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, *8*(6), pp.3140-3146.
19. Grimmelmann, J., 2004. Regulation by software. *Yale LJ*, *114*, p.1719.
20. Jacoby, D.L., 1960. Communication satellites. *Proceedings of the IRE*, *48*(4), pp.602-607.
21. Khan, O. and Estay, D.A.S., 2015. Supply chain cyber-resilience: Creating an agenda for future research. *Technology Innovation Management Review*, *5*(4).
22. Krause, D., Schwarz, E., Voinov, S., Damerow, H. and Tomecki, D., 2019. Sentinel-1 near real-time application for maritime situational awareness. *CEAS Space Journal*, *11*(1), pp.45-53.
23. Jin, Z., Azzari, G. and Lobell, D.B., 2017. Improving the accuracy of satellite-based high-resolution yield estimation: A test of multiple scalable approaches. *Agricultural and forest meteorology*, *247*, pp.207-220.
24. Lyall, F., 2015, February. The Role of Consensus in the ITU. In *Dispute Settlement in the Area of Space Communication* (pp. 33-42). Nomos Verlagsgesellschaft mbH & Co. KG.
25. Markopoulou, D. and Papakonstantinou, V., 2021. The regulatory framework for the protection of critical infrastructures against cyberthreats: Identifying shortcomings and addressing future challenges: The case of the health sector in particular. *Computer Law & Security Review*, *41*, p.105502.
26. Mazurelle, F., Wouters, J. and Thiebaut, W., 2009. The evolution of European space governance: policy, legal and institutional implications. *Int'l Org. L. Rev.*, *6*, p.155.
27. Oduntan, G., 2003. The Never Ending Dispute: legal theories on the spatial demarcation boundary plane between airspace and outer space. *Hertfordshire Law Journal*, *1*(2), pp.64-84.
28. Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K., 2001. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE control systems magazine*, *21*(6), pp.11-25.

29. Roberts, D.R., Paris, J.F., Manguin, S., Harbach, R.E., Woodruff, R., Rejmankova, E., Polanco, J., Wullschleger, B. and Legters, L.J., 1996. Predictions of malaria vector distribution in Belize based on multispectral satellite data. *The American journal of tropical medicine and hygiene*, *54*(3), pp.304-308.
30. Rosenfield, S.B., 1979. Where air space ends and outer space begins. *J. Space L.*, *7*, p.137.
31. Saha, S.S., Rahman, S., Ahmed, M.U. and Aditya, S.K., 2019. Ensuring Cybersecure Telemetry and Telecommand in Small Satellites: Recent Trends and Empirical Propositions. *IEEE Aerospace and Electronic Systems Magazine*, *34*(8), pp.34-49, 1.
32. Senior, K.L., Ray, J.R. and Beard, R.L., 2008. Characterization of periodic variations in the GPS satellite clocks. *GPS solutions*, *12*(3), pp.211-225.
33. Schmidt, D., Radke, K., Camtepe, S., Foo, E. and Ren, M., 2016. A survey and analysis of the GNSS spoofing threat and countermeasures. *ACM Computing Surveys (CSUR)*, *48*(4), pp.1-31.
34. Su, Y., Liu, Y., Zhou, Y., Yuan, J., Cao, H. and Shi, J., 2019. Broadband LEO satellite communications: Architectures and key technologies. *IEEE Wireless Communications*, *26*(2), pp.55-61.
35. Tankard, C., 2011. Advanced persistent threats and how to monitor and deter them. *Network security*, *2011*(8), pp.16-19.
36. Qu, Z., Zhang, G., Cao, H. and Xie, J., 2017. LEO satellite constellation for Internet of Things. *IEEE Access*, *5*, pp.18391-18401.
37. Wallis, T. and Johnson, C., 2020, June. Implementing the NIS Directive, driving cybersecurity improvements for Essential Services. In *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-10). IEEE.
38. Wu, W., Guo, F. and Zheng, J., 2020. Analysis of Galileo signal-in-space range error and positioning performance during 2015–2018. *Satellite Navigation*, *1*(1), p.6.
39. Wang, B., Liu, Y., Qian, J. and Parker, S.K., 2021. Achieving effective remote working during the COVID-19 pandemic: A work design perspective. *Applied psychology*, *70*(1), pp.16-59.
40. Weil, T. and Murugesan, S., 2020. IT Risk and Resilience-Cybersecurity Response to COVID-19. *IT Prof.*, *22*(3), pp.4-10.

EU and International Legislation

41. Commission Regulation (EC) No 912/2010 on setting up the GNSS Agency, OJ L 276/11, 20.10.2010.
42. Commission Regulation (EC) No 1285/2013 on the implementation and exploitation of European satellite navigation systems, OJ L 347/1, 20.12.2013.
43. Commission Decision 541/2014/EU on establishing a Framework for Space Surveillance and Tracking Support, OJ L 158/227, 27.5.2014.
44. Directive (EU) 2019/771/EC on certain aspects concerning contracts for the sale of goods, amending Regulation (EU) 2017/2394 and Directive 2009/22/EC, and repealing Directive 1999/44/EC, OJ L 136/28, 22.5.2019.
45. The Consolidated Version of the Treaty on the Functioning of the European Union (2007), Official Journal C 326, 26/10/2012 P. 0001-0390.
46. The Convention for the establishment of a European Space Agency (CSE/CS (37)19, rev.7), 30.05.1975.
47. UN (1967), *Treaty of Principles Governing the Activities of States in the Exploration of Outer Space, including the Moon and Other Celestial Bodies*, United Nations Office of Outer Space Affairs.

EU Documents

48. European Committee of the Regions. 132nd Plenary Session 5-6 December 2018. *OPINION. The space programme of the European Union and the European Union Agency for the Space Programme.*
49. European Commission (EC). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Space Strategy of Europe. Brussels, 26.10.2016.*
50. Commission Proposal (EC) for Regulation of the European Parliament and of the Council establishing the Space Programme of the Union and the European Union Agency for the Space Programme and repealing Regulations (EU) No 912/2010, (EU) No 1285/2013, (EU) No 377/2014 and Decision 541/2014/EU, 2018/0236 (COD).
51. European Commission (EC). *Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148.* Brussels.

52. European Commission (EC). *Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities*. Brussels, 16.12.2020.

53. European Commission (EC). *Communication from the Commission. Galileo. Involving Europe in a New Generation of Satellite Navigation Services*. Brussels, 10.02.1999

54. European Commission (EC). *Cooperation Declaration*- Digital Assembly 2019, Bucharest 13-14.6.2019

55. European Commission (EC). *Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade*. Brussels, 16.12.2020.

56. European Commission (EC). *Joint Communication to the European Parliament and the Council. Joint Framework on countering hybrid threats. A European Union response.* Brussels, 6.4.2016.

57. European Commission Directorate-General for Transport and Energy, *Midterm Evaluation of the Galileo project for the period 2002-2004. Final Report*, June 2006.

Online Sources

58. *Copernicus Overview.* European Space Agency. Retrieved from https://www.esa.int/Applications/Observing_the_Earth/Copernicus/Overview3, March 10, 2021.

59. *Galileo.* European Commission. Retrieved from https://ec.europa.eu/growth/sectors/space/galileo_en, March 10, 2021

60. *The Future is Quantum: EU countries plan ultra-secure communication network.* European Commission. Retrieved from https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network, March 10, 2021.

61. *Treaty of the Functioning of the European Union.* Eurofund, Retrieved from https://www.eurofound.europa.eu/observatories/eurwork/industrial-relations-dictionary/treaty-on-the-functioning-of-the-european-union, March 11, 2021.

62. *The History of the European Union.* European Union. Retrieved from https://europa.eu/european-union/about-eu/history_en , March 12, 2021.

63. *What is EGNOS?*. GSA. Retrieved from https://www.gsa.europa.eu/egnos/what-egnos , March 12, 2021.

64. *About Copernicus.* Copernicus. Retrieved from https://www.copernicus.eu/en/about-copernicus, March 12, 2021.

65. *Halloween Storms of 2003 Still the Scariest.* NASA. Retrieved from https://www.nasa.gov/topics/solarsystem/features/halloween_storms.html, March 14, 2021.

66. *Catalog of Earth Satellite Orbits*. NASA Earth Observatory. Retrieved from https://earthobservatory.nasa.gov/features/OrbitsCatalog, March 13, 2021.

67. *Boeing Satellites*. Boeing. Retrieved from https://www.boeing.com/space/boeing-satellite-family/, March 15, 2021.

68. *Space Economy at a Glance.* OECD. Retrieved from http://www.oecd.org/sti/futures/space/48301203.pdf, March 15, 2021.

69. *Galileo's Clock*- European Space Agency- Retrieved from https://www.esa.int/Applications/Navigation/Galileo/Galileo_s_clocks, March 19, 2021.

70. *The CubeSat Program*. CubeSat. Retrieved from https://www.cubesat.org/about/, March 20, 2021.

71. *CubeSat 101. Basic Concepts and Processes for First-Time CubeSat Developers*. NASA. Retrieved from https://www.nasa.gov/sites/default/files/atoms/files/nasa_csli_cubesat_101_508.pdf, March 20, 2021.

72. *Disrupting nation state hackers*. USENIX. Retrieved from https://www.usenix.org/conference/enigma2016/conference-program/presentation/joyce, March 16, 2021.

73. *Other Global Navigation Satellite Systems (GNSS)*. GPS. Retrieved from https://www.gps.gov/systems/gnss/, March 20, 2021.

74. *Low-Cost Satellite Market Size Will Grow Over USD 1 Billion During 2020-2024.* BusinessWire. Retrieved from https://www.businesswire.com/news/home/20210127006075/en/Low-Cost-Satellite-Market-Size-Will-Grow-Over-1-Billion-During-2020-2024-Wide-scale-Deployment-of-Secure-and-Reliable-Internet-Services-to-Emerge-to-Be-Key-Trend-Technavio, March 22, 2021.

75. *Earth Observation for Sustainable Development*. European Space Agency. Retrieved from https://eo4sd.esa.int/2020/06/01/eo4sd-water-products-catalogue/, March 22, 2021.

76. *Galileo is the European global satellite-based navigation system*. GSA. Retrieved from https://www.gsa.europa.eu/european-gnss/galileo/galileo-european-global-satellite-based-navigation-system , March 12, 2021.

77. *What was the space race?*. Space.com. Retrieved from https://www.space.com/space-race.html, March 24, 2021.

78. *NewSpace: The Emerging Commercial Space Industry*. NASA. Retrieved from https://ntrs.nasa.gov/api/citations/20160001188/downloads/20160001188.pdf, March 26, 2021.

79. *What is Spectrum? A Brief Explainer*. CTIA. Retrieved from https://www.ctia.org/news/what-is-spectrum-a-brief-explainer, March 26, 2021.

80. *Commission welcomes the political agreement on the European Space Programme*. European Commission. Retrieved from https://ec.europa.eu/defence-industry-space/commission-welcomes-political-agreement-european-space-programme-2020-12-16_en, March 29, 2021.

81. *Space Fact Sheet*. European Defense Agency. Retrieved from https://eda.europa.eu/docs/default-source/eda-factsheets/2018-09-21-factsheet_space.pdf, April 1, 2021.

82. *Strategic Context Cases (CCCs)*. European Defense Agency. Retrieved from https://eda.europa.eu/docs/default-source/eda-factsheets/2019-10-25-factsheet-scc, April 1, 2021.

83. *Iran `spoofed` US drone in order to land it*. The Jerusalem Post. Retrieved from https://www.jpost.com/Iranian-Threat/News/Iran-spoofed-US-drone-in-order-to-land-it, April 2, 2021.

84. *Annual Report 2020*. European Defense Agency. Retrieved from https://eda.europa.eu/docs/default-source/eda-annual-reports/eda-annual-report-2020.pdf, April 2, 2021.

85. *GNSS Authentication and encryption*. European Space Agency Navipedia. Retrieved from https://gssc.esa.int/navipedia/index.php/GNSS_Authentication_and_encryption, April 2, 2021.

86. *Why the Military released GPS to the Public*. Popular Mechanics. Retrieved from https://www.popularmechanics.com/technology/gadgets/a26980/why-the-military-released-gps-to-the-public/, April 4, 2021.

87. *EGNOS System*. GSA. Retrieved from https://www.gsa.europa.eu/european-gnss/egnos/egnos-system, April 6, 2021.

88. *Cybersecurity by design: building in the protection from the ground up*. Thales Group. Retrieved from https://www.thalesgroup.com/en/market-specific/critical-information-systems-and-cybersecurity/magazine/cybersecurity-design, April 6, 2021.

89. *Infrastructure overview*. Copernicus. Retrieved from https://www.copernicus.eu/en/about-copernicus/infrastructure-overview, April 6, 2021.

90. *Sentinel – 1.* European Space Agency. Retrieved from http://www.esa.int/Applications/Observing_the_Earth/Copernicus/Sentinel-1, April 6, 2021.

91. *Sentinel – 2.* European Space Agency. Retrieved from http://www.esa.int/Applications/Observing_the_Earth/Copernicus/Sentinel-2, April 6, 2021.

92. *Sentinel – 3.* European Space Agency. Retrieved from https://sentinel.esa.int/web/sentinel/missions/sentinel-3, April 6, 2021.

93. *Sentinel – 4.* European Space Agency. Retrieved from https://sentinel.esa.int/web/sentinel/missions/sentinel-4, April 6, 2021.

94. *Sentinel – 5.* European Space Agency. Retrieved from https://sentinel.esa.int/web/sentinel/missions/sentinel-5, April 6, 2021.

95. *A brief outlook on the future Copernicus Missions*. European Space Agency. Retrieved from https://sentinel.esa.int/web/sentinel/missions/copernicus-expansion-missions, April 6, 2021.

96. *Collaborative Ground Segment.* European Space Agency. Retrieved from https://sentinel.esa.int/web/sentinel/missions/collaborative, April 9, 2021.

97. *The Top 10 Hottest Satellite Companies in 2020*. ViaSatellite. Retrieved from http://interactive.satellitetoday.com/via/march-2020/the-top-10-hottest-satellite-companies-in-2020/, April 9, 2021.

98. *Collaboration Categories.* European Space Agency. Retrieved from https://sentinel.esa.int/web/sentinel/missions/collaborative/categories, April 9, 2021.

99. *Use Typologies and Available Services*. European Space Agency. Retrieved from https://sentinel.esa.int/web/sentinel/sentinel-data-access/typologies-and-services, April 9, 2021.

100. *Maritime data with unrivalled ocean coverage.* Spire. Retrieved from https://spire.com/maritime/, April 9, 2021.

101. *Malware.* The Independent IT-Security Institute AV-Test. Retrieved from https://www.av-test.org/en/statistics/malware/, April 9, 2021.

102. *Operating System Market Share Worldwide*. Statcounter GlobalStats. Retrieved from https://gs.statcounter.com/os-market-share, April 9, 2021.

103. *Europe's Spaceport.* European Space Agency. Retrieved from https://www.esa.int/Enabling_Support/Space_Transportation/Europe_s_Spaceport/Europe_s_Spaceport2, April 11, 2021.

104. *Federal data solutions*. Spire. Retrieved from https://spire.com/federal/, April 11, 2021.

105. *Actionable Satellite data for industry use cases from Iceye*. ICEYE. Retrieved from https://www.iceye.com/use-cases, April 11, 2021.

106. *Iceye SAR satellite orbits*. ICEYE. Retrieved from https://www.iceye.com/sar-data/orbits, April 11, 2021.

107. *Iceye SAR constellation capabilities*. ICEYE. Retrieved from https://www.iceye.com/sar-data/constellation-capabilities, April 11, 2021.

108. *Order Starlink.* Starlink. Retrieved from https://www.starlink.com, April 12, 2021.

109. *Security*, GSA, Retrieved from https://www.gsa.europa.eu/about/what-we-do/security, April 24, 2021.

110. *About GSA*, GSA, Retrieved from https://www.gsa.europa.eu/gsa/about-gsa#history, April 25, 2021.

111. *Internal Market, Industry, Entrepreneurship and SMEs. Space Research*, European Commission, Retrieved from https://ec.europa.eu/growth/sectors/space/research_en , April 25, 2021.

112. *Our History*. European Defense Agency, Retrieved from https://eda.europa.eu/our-history/our-history.html, April 27, 2021.

113. *Mission*, European Defense Agency, Retrieved from https://eda.europa.eu/who-we-are/Missionandfunctions, April 27, 2021.

114. *The new coronavirus could have a lasting impact on global supply chains*, The Economist, Retrieved from https://www.economist.com/international/2020/02/15/the-new-coronavirus-could-have-a-lasting-impact-on-global-supply-chains, April 28, 2021.

115. *The Cyber Threat to Satellites*, The Strategist, Retrieved from https://www.aspistrategist.org.au/the-cyber-threat-to-satellites/, May 3, 2021.

Other Sources

116. Aziz, A., 2013. The evolution of cyber attacks and next generation threat protection. In *RSA conference*.

117. EC, ESA, EDA. *Critical Space Technologies for European Strategic Non-Dependence. Actions for 2015/2017 V1.16*, March 2015.

118. Fleeman, E.L., 2001. *Technologies for Future Precision Strike Missile Systems-Missile Aeromechanics Technology*. GEORGIA INST OF TECH ATLANTA SCHOOL OFAEROSPACE ENGINEERING.

119. Reillon, V., 2017, *European Space Policy. Historical perspective, specific aspects and key challenges*, European Parliamentary Research Service.

120. Thomas, J., 2001. Ethics of Hacktivism. *Information Security Reading Room*, *12*.

121. Unal, B., 2019. *Cybersecurity of NATO's Space-based Strategic Assets*. Chatham House. The Royal Institute of International Affairs.