CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Security Studies

Master's Thesis

2023 **Bc. Tomáš Kouba**

CHARLES UNIVERSITY

FACULTY OF SOCIAL SCIENCES

Institute of Political Studies

Department of Security Studies

Prevention of threats to Galileo Global Navigation Satellite System

Master's thesis

Author: Bc. Tomáš Kouba

Study programme: Security Studies

Supervisor: Mgr. Bohumil Doboš, Ph.D.

Year of the defence: 2023

Declaration

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

In Prague on May 3, 2023 Tomáš Kouba

References

KOUBA, Tomáš. *Prevention of threats to Galileo Global Navigation Satellite System.* Praha, 2023. 78 pages. Master's thesis (Mgr.). Charles University, Faculty of Social Sciences, Institute of Political Studies. Department of Security Studies. Supervisor Mgr. Bohumil Doboš, Ph.D.

Length of the thesis: 168 419 characters with spaces

Abstract

This diploma thesis presents a single case study exploring how the Galileo Global Navigation Satellite System (GNSS), a European autonomous navigation system, deals with threats. Space systems nowadays face many types of dangers including electronic, cyber, kinetic physical, directed energy or natural attacks. At this point, since Galileo GNSS is one of the most advanced technologies that is also considered to be a strategic one (for EU and ESA), it is important to reveal and describe the system's vulnerabilities to external material or technical threats. This diploma thesis describes the history, development, current situation and position of Galileo GNSS on the global scene. Furthermore, this thesis will summarize the possible material threats to space objects and finally operationalize them to the conditions of Galileo. The prevention measures identified as insufficient or improvement-worthy are then presented with recommendations for possible future development or enhancing factors which would increase Galileo's strategic service (PNT) safety.

Abstrakt

Tato diplomová práce se věnuje globálnímu družicovému polohovému systému Galileo, autonomnímu evropskému navigačnímu systému, a hrozbám, kterým čelí. Systémy působící ve vesmíru jsou v dnešní době pod tlakem mnoha možných hrozeb včetně elektronických, kybernetických, kinetických, nekinetických útoků nebo přírodních pohrom. Galileo je jednou z nejpokročilejších technologií, kterou lze také označit jako strategický zdroj informací a dat pro EU a ESA. Je tak důležité odhalit a popsat dané hrozby z pohledu technologie, kvůli kterým může být systém poškozen nebo kvůli kterým může být zranitelný a daná data tak v ohrožení. Tato diplomová práce pak představuje historický vývoj, následně současnou situaci a postavení systému Galileo ve světě. Dále jsou shrnuty možné hrozby pro objekty ve vesmíru, které jsou nakonec použity v podmínkách Galilea a vyhodnoceny v rámci dostatečnosti preventivních opatření. Pro ta opatření, která jsou vyhodnocena jako nedostatečná, jsou následně předložena doporučení pro možný budoucí vývoj nebo postupy pro samotné preventivní úkony, které by zvýšily bezpečnost služeb poskytovaných satelitním systémem Galileo (PNT).

Keywords

Galileo, GNSS, European Union Agency for the Space Programme, EUSPA, European Space Agency, ESA, space debris, cybersecurity

Klíčová slova

Galileo, GNSS, Agentura Evropské unie pro kosmický program, EUSPA, Evropská kosmická agentura, ESA, kosmické znečištění, kyberbezpečnost

Title

Prevention of threats to Galileo Global Navigation Satellite System.

Název práce

Prevence hrozeb pro globální družicový polohový systém Galileo.

Acknowledgement

I would like to express my gratitude to my thesis supervisor, Mgr. Bohumil Doboš, Ph.D. for his valuable advice, comments, willingness and time he gave me in writing this thesis; and also to my relatives and friends who supported me all this time.

Table of Contents

Introduction

The new globalized world is a place where all processes are technologically interconnected. Space technology is not an exception to this fact, as space is estimated to become one of the main domains of the future in terms of exploration, technology, civilization development, and mainly as economic accelerator. Global navigation satellite systems are crucial for a vast number of economic and industrial fields that rely on the data provided by the satellites to the final user's devices. The usage of these systems extends beyond individual navigation and includes all autonomous systems, such as self-driven cars or autopilots. Every single person and every single company within industrialized society relies on positioning, navigation and timing (PNT) services. If those services would become unavailable, the economies of the world would begin slowing down and collapsing, air transport would stop working in seconds and military actions in terms of predictability and defensive measures would become way harder.

PNT is not a technology that can be easily substituted or replaced by a different invention. Not only the globalized and interconnected economies, but also the post-modern society as a whole are dependent on positioning, navigation and timing services provided by GNSS. National security as we know it is born from the PNT invention and development in the past decades. Galileo GNSS came onto the scene with a vision of making the European countries independent of other states' decisions regarding the respective service provision. With this goal in mind, Europeans made the most accurate and developed system from all the available global navigation satellite systems (and the system is still under developmental improvement (ESA, 2023) which serves not only the governments, but primarily the people as the only civilian-controlled project of GNSS with global coverage and high accuracy (Lindström and Gasparini, 2003).

The European Union took the road of developing its own satellite navigation system despite being given the chance to cooperate on GPS (U.S.) or GLONASS (Russia) systems. When the conflict in Ukraine broke out in February 2022, this decision was commended in terms of freeing and defending the European countries from the influence of their eastern rival in Russia. As history has proven time and time again, intercountry relations are unpredictable at best. A partner today may be suddenly cut off tomorrow. The terms of the U.S. deal were not acceptable benefits of their system co-development participation, Russian participation was left for the satellite-carrying equipment and

cooperation with China ended with failure resulting in alienated know-how (European Commission, 1999; Nouwens and Legarda, 2018). Even if the benefits and costs were evaluated for all possible partners, the opportunity to strengthen the EU's independence and strategic position in space activities, develop a new branch of the inbounds industry with thousands of newly created jobs and highlight the technological innovation of Europe significantly outweighed all other arguments. This goes hand in hand with the EU's strategic autonomy concept, which highlights the need for the capacity of the EU to act autonomously and cut off the dependency on other countries in the strategic sectors, sectors such as the global navigation capability.

However, the strategic power of such technology also brings about challenges to its operation, specifically in terms of preventing harm that would affect not only the device, but also the economy, health system, transportation, and people's day-to-day lives. This thesis aims to highlight the possible challenges and threats to the Galileo Global Navigation Satellite System and find answers on how to deal with the threats which can ruin the idea of safe, accurate and independent positioning, navigation and timing service. The primary focus of this thesis will be to elaborate in detail on the open-access information and literature inspired by the development of Galileo GNSS, technical (material) threats to GNSS in general and finally the defence mechanisms of Galileo GNSS. This approach must then be considered as a case-specific study linked to the conceptualization of the possible technical (material) threats through threat modelling. Individual points of the thesis are divided into separate chapters and subsections which will unite and connect the understanding of Galileo and recognized threats to space systems. The individual elements will then be analysed, and outcomes will be presented in recommendations and conclusions.

First of all, the thesis will develop the conceptual framework and methodology as a key aspect of the analysis. The development and in-detail description of the Galileo Global Navigation Satellite System will be outlined in the first part of the thesis itself to better understand the technology and current situation. Threats to GNSS are also key elements that will follow with their function, occurrence, and danger description. As the next crucial part of this thesis, the threats will be operationalized and applied specifically to the Galileo GNSS with elaboration on the open-access information regarding prevention or defending measures that are actively used. Finally, all the findings will be tied in a

conclusion and recommendations for threats which are objectively underestimated, if any, and the research questions and hypothesis answered.

The conceptual framework is divided into three sections – GNSS, possible threats to space systems and threat modelling. The first section, basic information on GNSS and a brief introduction of the topic, builds upon the work of Richard B. Langley, Peter J. G. Teunissen and Oliver Montenbruck and their *Introduction to GNSS,* a chapter within *Springer Handbook of Global Navigation Satellite Systems* (editors P. J. G. Teunissen and O. Montenbruck, 2017). Threats to space systems and their conceptualization are then inspired by Todd Harrison's *Escalation and deterrence in the second space age* (co-authors Z. Cooper, K. Johnson, T. G. Roberts, 2017). Finally, threat modelling is a concept by A. T. Sheik and a collective published and elaborated in *Advances in Space Research* (2022). An important part of the thesis is of course the methodology approach that is inspired by a case study by J. Gustafsson (2017) and M. Hennink in *Qualitative Research Methods* (2020). The primary sources of the history and development of Galileo GNSS are pieces by Javier Pérez Bartolomé et al. in *Overview of Galileo System* (2015) and official information from the European Space Agency (ESA), European Union Agency for the Space Programme (EUSPA) and European GNSS Service Centre (GSC). The second chapter's threats to space systems are sourced mainly from aforementioned Todd Harrison's work and Spirent's (leading telecommunication company) white papers. Finally, the operationalization of threats is inspired by official information from the EU officials, ESA, EUSPA, GSC or the United Nations Organization. The information is then gathered from multiple sources and crosschecked with additional secondary sources to provide the most accurate information regarding the elaborated topic. Recommendations are then based on findings revealed throughout the thesis and improvements for the available options on how to optimize the prevention and security measures.

Conceptual Framework

As the first step to reveal the individual parts of the thesis, it is important to define and understand what the Global Navigation Satellite System is, or how to understand a threat. Additionally, threat modelling should also be highlighted as one of the key concepts for this thesis since some of the threats are just described as 'what could happen' (not experienced) if the technology will not be able to prevent it.

Global Navigation Satellite System

Global Navigation Satellite Systems (GNSSs) are high-technology pieces which members of post-modern society rely on in their everyday lives. GNSS is a satellite network which is responsible for positioning, navigation and timing (PNT) services based in outer space. Even if it is easily predictable, the constellation of satellites is not the only part of the system since the satellites 'only' broadcast the signal which is transmitted to Earth. Such technologies are heavily supported by the ground-based facilities which operate the service. The transmitted signal then indicates where the receiver is at what time. The accurate position is then provided by at least four satellites which 'see' the receiver and through complex algorithms provide the data (Novatel, n.d.).

The development can be traced back to the 1950s and 1960s when optical and radio techniques started to be used as a space-based system. Nowadays, the technology is significantly developed and different at the same time, but the goal was preserved as the provision of PNT services. Current Global Navigation Satellite Systems (GNSSs) but also Regional Navigation Satellite Systems (RNSSs) usually consist of three segments: space, control, and user. The space segment is then the one above the Earth's surface consisting of a constellation of satellites in outer space. The control system is responsible for keeping the system functional and monitoring the signal broadcast. Finally, the user system consists of the signal-receiving equipment for performing the service. In addition to it, GNSSs' constellation of satellites is usually based on a medium-altitude orbit (MEO) configuration which secures the highest performance for global coverage. For the regional ones, geostationary orbits (GEO) are sufficient as they are monitoring still the same area (Langley et al., 2017).

There are 6 significant Global or Regional Navigation Satellite Systems nowadays. GPS (US), GLONASS (Russia), BeiDou (China) and Galileo (EU) are those which operate globally. QZSS (Japan) and IRNSS/NavIC (India) operate with regional coverage (Langley et al., 2017).

In addition to the essential PNT service the GNSS constellations provide, there are also minor services which can enhance the competitive capabilities of the individual systems such as BeiDou's Short Message Service or Galileo's Search and Rescue service. The first mentioned helps its users to send short messages even if the mobile communication signals are damaged or the area is not covered, which can help during emergency events

such as earthquakes. For Galileo, the Search and Rescue service transmits distress signals to the relevant authorities and locates the people sending them. Additionally, Galileo messages the distressed back about receiving the request (Inside GNSS, 2021; EUSPA, 2023a). Moreover, Galileo in cooperation with QZZS are developing the GNSS Emergency Warning Service which should enable it to locate an emergency and address the alerting messages to everyone in the perimeter with instructions based on the zone the individuals are located in. This service will greatly aid governance during emergency situations (GSC, n.d.a).

Threats to space systems

As for the purpose of the thesis, technical (material) threats to space systems are not limited only to outer space, but can also target the facilities that operate from the ground or provide communication between ground and space segments. The threat is then considered as an act or situation which can intentionally or unintentionally change the performance of the technology. Since unintentional threats are usually generalized as of natural origin with a lack of prevention measures, intentional are those that are man-made and usually tend to affect the system. Such threats, if realized, typically endanger communication and transport streams with huge effects on global health, positioning, navigation, and timing, and mean losses in billions of EUR or USD every single day (Harrison et al., 2017).

Threat modelling

As the space segment is not easily reachable by any individual who would think of an attack against the GNSS system, some of the presented threats are modelled towards prevention measure development rather than based on previously experienced attacks. While there have been many cases of previous threats, preventative measures have already been put into place based on the known cases of the system and service disruption. The rest of the presented threats are hypothetically achievable and the response or prevention to them are rather estimated or calculated from the modelling experience. Threat modelling is a basic requirement for modern technologies that are widely used and provide some sort of service to the final users. In the case of space systems, this technology is additionally super expensive and any underestimated threat which would come true would mean an economic and functional disaster (Sheik et al., 2022).

Threat modelling is widely used and known in the field of IT and cyber security measures. Its focus lies in the identification of a possible threat and modelling of its performance if it would come true. This model serves for setting prevention and security provisions on how to limit the effect or shut down the threat. Its goal is to reduce the risk of the feasibility of the threat and its outcome if the threat occurs (Torr, 2005). In the case of space technologies and systems, threat modelling can be understood as a still ongoing process because the systems are being developed even during the time of their service provision. At that point, the threats which were conceivable at the time of developing the satellite – the object itself – do not have to be accurate. The system must be tested all the time and follow the 'trends' mainly in the field of non-kinetic threats – cyber security and cyber attacks threats (Sheik et al., 2022).

As per the presented evidence, some of the threats outlined in this thesis are conceivable so the appropriate response in the means of prevention measures must be modelled since the systems are not 'one-time use' and are not easily substitutable. The process of preventive mechanisms invention is a step-by-step modelling of a threat, which is presenting the possible attack, convincing the audience of its feasibility, and then consequently looking for a solution to solve the problem and prevent its occurrence or effect (Shevchenko et al., 2018).

Methodology

As the thesis focus lies in a case-specific field elaborating on the Galileo Global Navigation Satellite System, the main methodology approach is a single case study. This case study will then focus explicitly on only the Galileo GNSS because such systems benefit from specific scrutiny. Galileo GNSS is a unique global system that affects billions of people, and it is not a template for all the other navigation systems, so this thesis' result cannot be used widely over all other GNSSs (Gustafsson, 2017; Hennink et al., 2020). At the same time, since Galileo is compatible with GPS and other systems (depending on software and receivers), some aspects might overlap. In general, since the main focus is on Galileo, this diploma thesis will not tend to generalize the applicability of the outcomes for other systems, even if the recommendations could be applicable to more than just Galileo. It is also important to mention that even if Galileo GNSS has an Open Service and Public Regulated Service with different types of security measures, this diploma thesis will focus on the lowest secured level – Open Service – as it is the one which is accessible to ordinary users.

As presented before, this thesis will focus on the prevention of threats from the material-technical point of view and avoiding immaterial political or economic threats, so threat modelling is a key part of the investigation as a crucial concept for threats that were never experienced directly against satellites but are considered to be feasible ones (i.e., nuclear attacks). The focus on technical (material) based threats is mainly due to the need to hone the scope of this thesis to make it both understandable with an in-depth recognition of the material threats and solutions, while keeping the thesis to in an acceptable length. In addition, this thesis aims to present the visible threats which can be recognized and prevented in physical or technical ways. Political or economic threats are also essential for projects such as Galileo, but their prevention measures would be much more abstract without clear physical tools to mitigate them. Technical (material) threats are those that can be most precisely described, their effect is visible and immediate, and the human factor is limited only to the initial point.

The thesis is expected to bring answers to three set research questions. The first and the most comprehensive is: *How do the European Union Agency for the Space Programme (EUSPA) and European Space Agency (ESA) deal with possible threats to Galileo GNSS?* The answer to this research question will be based on the open-access information and analysis of Galileo GNSS, available threats and EUSPA's and ESA's provisions for prevention the of possible harms.

The second research question tends to evaluate the prevention measures and asks: *Is the security of Galileo GNSS prevention sufficient?* Based on the answer to the first research question and revealed details of the system and threats, the data must be compared to already experienced threats in action and the effectiveness with which Galileo dealt with them.

The last research question is: *What should be done more to prevent any harm to the operationalisation of Galileo GNSS?* The answer to the final research question then aims to propose recommendations for improving security and preventive measures if the answers to the previous questions are fully or partially negative in any field.

Finally, the recommendations presented at the end of this thesis are based on the findings of the previous sections and are suitable for soliciting solutions for the underestimated threats. These described recommendations are then answers to the identified

improvement-worthy security measures which could potentially help to deal with lowering the risk of attack or harm caused by a certain threat.

All the research questions will be then evaluated, and the outcome should confirm or disprove the settled hypothesis: *Galileo GNSS is sufficiently secured against external threats*. To set boundaries which can measure if the system is sufficiently secured is to determine how Galileo is dealing with the presented threats and whether the best available technology and security measures have been implemented for Galileo GNSS. The sufficiency must be considered in terms of achievability because if the understanding should shift into solely theoretical, there would be always something to be invented for enhancing the security measures. For evaluating the sufficiency, it is important to determine whether all the presented threats have any pre-existing effective counter-solution or if the missing solution is already achievable but not implemented on a Galileo basis. If the provided description of current prevention measures is concluded to be predominantly effective, or if any solution is not yet available but the threat is also not at the stage that it would harm the GNSS satellite constellation (intentional threats), the individual outcome can be considered as currently 'sufficiently secured'.

This thesis will rely on open-access information about the Galileo GNSS from the official sources of EUSPA, ESA, and EU as well as already published scientific examinations of Galileo's performance. As for other aspects of the thesis, professional and scientific publications, scientific articles, and accessible government documents will be used, as well as secondary sources in cases of lack of publications on the specific theme.

1 Galileo Global Navigation Satellite System

Galileo is a European leading space program operated by the European Union Agency for the Space Programme (EUSPA). The idea of an autonomous navigation system was already in the minds of many in the nineties when the European space program started accelerating. The main goal was to bear away from the full dependence on the United States of America and its well-known GPS navigation system. Nowadays, Galileo serves billions of people and thousands of companies with accurate positioning information and navigation services, with the target of being considered the most precise navigation system. The goal is to perform location and navigation services to all European public and military authorities independent from any other constellations operated by different regional hegemons such as the U.S., Russia or China. At the same time, Galileo tends to enhance its service to other parts of the world thanks to its compatibility with the U.S. GPS, which supports its global plans. Even if Galileo has its own global coverage, its interoperability with GPS allows it to continue to perform precise positioning and navigation information.

1.1 History and development

Navigation and positioning services started to be really crucial in the late 20th century. Like most geographical areas, the European sector was fully dependent on the U.S. GPS non-civil system and Russian GLONASS. As the Cold War escalated, the desire for independence from the decisions of other countries arose. At the early stage, the program was not meant to be fully separate from the other navigation systems. GNSS-1, the first stage of development, was operated by the European Space Agency (ESA). This part of the development was also meant for the deployment of regional space facilities across the European Union. GNSS-2 was a continuing part of the process when it was enhanced into global system intention. The idea of a separate European navigation system then faced several discussions over the system's aim, including whether an autonomous system was necessary, or if an augmentation system for GPS would not be enough. The final agreement on the development of GNSS-1 was concluded on the 18th of June 1995 between executives of ESA, the European Community and Eurocontrol (European Organisation for the Safety of Air Navigation). At that time, the GNSS-1 was officially named to European Geostationary Navigation Overlay System (EGNOS) with the primary aim to build and develop a satellite-based augmentation system which should serve as a supportive infrastructure for GPS and an improvement tool for air navigation

in Europe and the adjacent area. In the mid-nineties when GPS became fully operable, the U.S. government finally committed to providing GPS geolocation service to the civil population. At that time, GNSS-2 (later named Galileo), started to appear in discussions over an autonomous navigation system fully independent of GPS and any other providers out from the European Union. The reason was simple – the U.S. could easily downgrade the GPS accuracy, limit accessibility or even select availability for certain areas and users at a whim. Even if the EU and the U.S. were close allies at that time, the uncertainty of the future manipulated and accelerated the decision over a new GNSS based in the EU. The debate over autonomous GNSS was formally opened in 1998 by the European Commission publishing *Towards a Trans- European Positioning and Navigation Network: including a European Strategy for Global Navigation Satellite Systems (GNSS)* where this need was expressed (Bartolomé et al., 2015). This communication directly mentioned that the European Union should not step back in technological development, and it is a question of a strategic measure to control its own GNSS system. The call for its own strategic GNSS project was also recognized in the resolution from the European Parliament concluded in 1999 (European Parliament, 1999).

Later in 1999, the European Commission in cooperation with ESA officially stated their strategic aim to develop the Galileo program which would secure and provide a positioning system for European users who would not be affected by any other third country's (outside of the EU) change of policy. The key point was to decide which of the three ways of development to take:

(1) a joint global system;
(2) EU's cooperation in development with the U.S. or Russian Federation;
(3) independent development of the EU's own system.

As investigated by the Commission, the U.S. side was willing to cooperate under the condition of acceptance of their own GPS standard positioning system and later fully rejected from their side as a 24-satellite-based system plan was revealed. The U.S. could not accept such a wide constellation with regards to military considerations. Overall, future cooperation between the two satellite systems was confirmed for civil purposes. For the Russian side, there was a huge advantage of taking the know-how from their existing GLONASS system. EU first accepted the second round of negotiations on a strategic partnership for the development of this system. Later, the Russian credit was left

for using their rockets to bear the Galileo satellites into space (European Commission, 1999; Zervos and Siegel, 2008).

The so-called 'Zero option' – where the EU would decide to not continue with the proposal of the Galileo system and remain reliant on the non-member country system – was strictly rejected. Even if the public spending and funding of the project were considered to be extremely burdening, the arguments for the need to preserve the EU's values (political, economic, strategic etc.) outweighed the potential complexity and time-burden of the project itself. As Galileo was meant not only for civil purposes, but also to cover the safety requirements in the developing world after the end of the Cold War, the zero option conditions were seen as little more than an idyllic dream. Developing a system similar to Russian GLONASS or American GPS was another opportunity for the EU body and many member countries expressed interest in cooperating on such a project to tie connections between member states in terms of research and employment. Successful program outcomes would also serve as open grants to all participants that could take advantage of new discoveries and inventions for state holders, and the private sector would be able to participate in this public-private partnership. At this early stage, European Commission strongly expressed its willingness to be fully compatible with GPS, open and global, but fully independent from any other present and future existing navigation systems (European Commission, 1999).

The European Space Agency conducted *Galileo Sat Study* in November 1999 which initiated the first phase of the Galileo project. One year later, the GPS Selective Availability was removed, which the EU understood as an attempt to make the Galileo project useless. On the contrary, the EU strongly showed its support for their future navigation system (even if the Ministers asked for further information and documentation later due to dissatisfaction from public-private cooperation and problems with management structure). In the meantime, limited development was approved for Galileo, and the EU's main body funding was frozen until questions were answered. At this time, ESA had already committed their share of EUR 550 million in November 2001 to fund at least the limited development, and they waited for the final approval from the Ministerial Council (Bonnor, 2011).

The peak in decision-making for Galileo should have come in the meeting in December 2001 when the EU Ministers of Transport discussed the proposal. Unfortunately, the

agreement was not concluded and the official initiation and funding from the EU side were not confirmed due to a need for further expertise on economic perspectives. As for the initiation, officials released EUR 100 million to keep the project alive. The agreement was finally reached in March 2002 and the remaining funds (EUR 450 million) were released. As for the place of a project-leading country, Germany and Italy tried to outbid each other (which would consequently harm the feasibility of the project). Finally, an agreement was concluded for mutual inter cooperation (Bonnor, 2011). Additionally, cooperation with other third-country actors was investigated and finally signed between the EU and China over scientific and technological development in 2003. By that time, China proposed to partially fund research for the Galileo project to help its own small-scale regional satellite system BeiDou (later developed into another GNSS). From the very beginning, there was open scepticism from the U.S. regarding China's involvement in such a strategic project, mainly due to technology transfer from the EU to China, which endangered U.S. interests. In 2010, the Chinese parts incorporated into the planned launches of Galileo satellites were de-assembled and cooperation was ended (De Selding, 2010; European Commission, 2003; Matias, 2007).

In the early 2000s, there was an agreement on specificities of signal design, code selection, spectrum allocation, frequencies and other high-technology communication basic settings. Therefore, Galileo's frequency plan was protected by the World Radio Communications Conference (held in June 2000) until June 2006 (Bartolomé et al., 2015). Four years later, in 2004, the EU and U.S. representatives achieved an agreement on Galileo and GPS cooperation plan and their interoperability and compatibility (Bonnor, 2011).

From the point of view of NATO, the newly brought idea of the Galileo system provided several possibilities to the alliance. The combination of GPS and Galileo signals would provide greater reliability of information and data to military receivers. This would be mainly beneficial in urban areas with insufficient coverage of GPS satellites and the possibility of a loss of precise PNT data. EU member states of NATO then would have a more effective role under the alliance's command. On the other hand, a conflict of interest between the non-NATO EU members could arise over the usage of Galileo during military operations (Lindström and Gasparini, 2003).

As the new satellite system was meant to be fully autonomous and no strategic partnership was concluded at the start, the development itself took several years before it could reach the stage of usability. This is also linked to the structure of the technology since Galileo should be a huge global system based on precise positioning. One of the key components of the satellites is Rubidium Atomic Frequency Standard (RAFS) and Passive Hydrogen Maser (PHMs) also known as the atomic clock to control the frequency (Bartolomé et al., 2015). The atomic clock ensures that the signals broadcast from and towards the satellite are transmitted synchronously and the information the receiver gets is accurate. Its accuracy is expressed in the loss of seconds in a certain period of time. In the case of the rubidium atomic clock, it would lose only three seconds in one million years. For the PHMs, they would lose two seconds in three million years. On the other hand, the latency of just a few nanoseconds would cause an error in positioning that would be recognizable in a couple of metres on Earth (ESA, n.d.a). The development of these atomic clocks was launched in the late 1990s to be integrated into future satellites and in the early 2000s recognized as on-ground qualified (Bartolomé et al., 2015).

Usually, when a new technology is about to be launched, there are several tests on its operability. The European Space Agency started a Galileo System Test Bed 1 program (GSTB-V1) in 2002 which aimed to develop a ground-based segment which would validate Galileo algorithms and products based on measurements from GPS. One year later, in 2003, the ESA began development of two prototypes of the satellites under marks GIOVE-A and GIOVE-B. This was part of the GSTB-V2 program which followed after the first one (Bartolomé et al., 2015).

Galileo In-Orbit Validation Element-A (GIOVE-A) was the real first step towards to the operationalization of the European navigation space program and also the first element of the validation phase. This satellite was launched in December 2005 less than 30 months after its announcement. Such a short time and its final success demonstrated that even low-cost and rapid-response technologies can be used for difficult and ambitious programs such as Galileo. This was something brand new in comparison to other navigation systems such as GPS and GLONASS validation processes. On the occasion of the launch, Russian credit and cooperation were measurable since the satellite and spacecraft GIOVE-A were launched at Baikonur Cosmodrome, Kazakhstan, which serves as the main launching area rented by Russia. The goal of the mission was to verify the accuracy, generate the first Galileo navigation signals in space, test the rubidium atomic

clock in space and demonstrate the operability in the radiation environment of the Medium Earth Orbit (MEO) where Galileo should operate (Kramer, n.d.a). The major success of the GIOVE-A was achieved in January 2006 when the Galileo-like signal in space was transmitted for the first time from the orbit to the Earth. This fulfilled the frequency protection given by the International Telecommunications Union which had validity until June 2006 (Bartolomé et al., 2015). GIOVE-A's lifetime was designed for 27 months but since it performed excellently, it was prolonged multiple times and continued operating for 78 months. The GIOVE-A mission was officially terminated in 2012 by ESA but was still actively used by its constructor Surrey Satellite Technology Ltd (SSTL). SSTL successfully decommissioned the GIOVE-A satellite in 2021 (Kramer, n.d.a).

Galileo In-Orbit Validation Element-B (GIOVE-B) was launched into space in April 2008 after several delays with the main aim to test the technology which was needed for the Galileo constellation. The satellite reached MEO and started transmitting the first navigation signals in early May 2008. This was a great achievement since this was the first time when the satellite transmitted the GPS-Galileo common signal Multiplexed Binary Offset Carrier modulation (MBOC) specifically optimised for future cooperation between the EU and U.S. governments on navigation systems. In the summer of 2009, GIOVE-B achieved the main goal of maintaining the Galileo frequencies. This also confirmed that the EU has the most accurate atomic clocks among all the other actors in space – the PHMs. In 2011, the lock was still the most precise in space (until the first official Galileo satellite reached orbit later). ESA ended an incredibly successful mission of GIOVE-B in July 2012 in paving the path for the Galileo-meant satellite constellation (Kramer, n.d.b).

The early development and validation phase demonstrated the excellent condition of European engineering in the space exploration and technology field. At this point, two main Galileo implementation phases occurred. *The In-Orbit Validation phase* (IOV) was the first one that aimed to validate the end-to-end Galileo service concept in the constellation of four operational spacecraft and a minor ground-based infrastructure system. The second one, *The Full Operational Capability phase* (FOC), aimed for the full constellation and operability of the Galileo satellites. The FOC phase should achieve the full ground and space-based system with full validation and excellent service performance of the Galileo constellation (Bartolomé et al., 2015).

The IOV phase contained two launches of four satellites (2 + 2) which should validate Galileo's geolocation operability and cooperation between space-based, ground-based and user-aimed technology. The first pair of satellites (FM1, FM2) was launched in October 2011 from the European Cosmodrome in French Guyana and started operating after months of testing conducted by ESA and private-based companies cooperating on the program. The start was delayed by one day because of a problem with the ground-support fuelling system. This was also a historic moment from the point of view of the EU-Russian cooperation since it was the first time when a Russian spacecraft lifted off from the European spaceport and even more, the first Soyuz launched outside of Russia (Plesetsk) or Kazakhstan (Baikonur) (GPS World, 2011). The second pair of Galileo's IOV satellites (FM3, FM4) was launched one year later in October 2012 from French Guyana with multiple delays. After a series of tests, they joined the IOV constellation of four satellites in total (FM3 and FM4 included) and started transmitting a signal as a part of the validation phase for the Galileo system (Aerospace Technology, 2012).

The process of in-orbit validation was achieved in 2014 when the navigation services were performed with extraordinary accuracy considering that there were only 4 satellites in orbit. The process of validation began in March 2013 when the second pair of IOV satellites reached the constellation and interconnected with all the components. As four satellites are the minimum number of 'devices' to perform navigation services, interconnection enabled testing of the full Galileo constellation before the Full Operational Capability was about to be launched. The result of this phase was that Galileo worked and performed well with the accuracy of 8 metres horizontally and 9 metres vertically 95 % of the time. Moreover, as long as more satellites are launched into orbit, the accuracy gets more precise (GPS World, 2014).

Once Galileo project was finally alive and brought onto the scene, several targets which should have been met by its implementation of the project were recognized including political, economic, and technical challenges. From a political standpoint, Galileo gave Europeans an effective instrument of sovereignty from other key actors in the sector (mainly the U.S. and Russia), deepened European interaction between the key stakeholders and tied relations over a strategic project with a global impact which also brought a challenge to achieve a strong position on the international scene. Addressing the security implications of Galileo was also set as one of the key political challenges. In the field of economic challenges, the creation of a cost-effective organization running the

project with a public-private sector partnership opening a new European market was one of the main goals. Finally, technical challenges were represented by the exploitation, evolution, and implementation of a fully operational global system with the highest accurate achievable data provision. Interoperability and compatibility with other currently available systems were then set as goals for the promotion of the globalized world which would deepen international actors' relations and provide the highest service effectivity of the Galileo system (Sitruk and Plattard, 2017; Stephenson, 2012).

1.2 Current situation

The Full Operational Capability should consist of 30 MEO satellites (24 active + 6 spares carried by three orbital planes/8 active + 2 spares each spread evenly around the plane). This was set to cover every place in the world at any time with at least four satellites' view, but most of the time six to eight satellites cover every area at any moment, providing the most accurate positioning service available (in scale of centimetres). The inclination of satellites is set for 56° which also secures the coverage of the polar areas which are poorly monitored by other navigation systems. Moreover, in areas which are highly populated, interoperability with the U.S. GPS raises the accuracy of the system (ESA, n.d.b).

As the prototypes and validation phases went well, further planning took action and the decision on the provided service was at the spot. In the beginning, there were 3 identified services which Galileo provided:

(1) Open Service (OS)
(2) Public Regulated Service (PRS)
(3) Search and Rescue Service (SAR)

The Open Service is designed to serve the wide public free of charge in positioning and timing information (Bartolomé et a., 2015). All the devices with the needed incorporated Galileo-compatible navigation receiver (more than 95 % of electronic devices nowadays such as telephones or in-car navigations are equipped with such a tool) are in possession of the service. This service was switched from the testing phase to the provision of life services in January 2017 with additionally declared evolution when the Full Operational Capability will be reached (EUSPA, 2016).

The Public Regulated Service is designed to provide positioning and timing information for government-authorised users, which means that the signals will be encrypted based on the PRS security module with an incorporated decryption key. These services are provided at any time no matter what circumstances are in the world. Its operability is one of the strategic aims due to the importance of the provided information (ESA, n.d.c).

The Search and Rescue Service is an objective contribution to international cooperation in humanitarian aims such as search and rescue. The FOC should secure the improvement of the so-far implemented system in speed and accuracy of the signal in cases of humanitarian operations (ESA, n.d.c).

There were also ideas about (4) Commercial Service (CS) when the Full Operational Capability of Galileo services would be reached. This decision to implement Commercial Service was finally adopted in 2017, later renamed to High-Accuracy Service (HAS) and stated to be free of charge (EUSPA, 2017). This service will be provided once the FOC is achieved and will be targeted mainly to private and public sector companies for their strategic aims of using space technologies for improving their service. This will be achieved by Precise Point Positioning (PPP) where the positioning accuracy is less than 20 cm in a coverage time of fewer than 300 seconds worldwide. In the European area, the coverage time should be downsized to less than 100 seconds within the same positioning accuracy of less than 20 cm (GSC, n.d.b).

There was also a plan for a Safety-Of-Life service (SOL) which should increase the safety of the traditional non-ground-based infrastructure services targeting airlines and maritime companies on a global scale. As for the purpose, it would use the frequencies reserved for Aeronautical Radio-Navigation Services (ESA, n.d.c). This service planning was postponed until further notice, to be revisited once the later phases of Galileo constellation operability are achieved (Bartolomé et al., 2015).

The number of FOC satellites in the constellation changed from the time when the Safety-of-Life idea was at the very beginning. At the start, there were planned to be 27 operational satellites in MEO. Finally, in 2012 the plan was changed to 24 operational satellites after several analyses proved that the lower number will also meet the requirements for availability and accuracy. The semi-major axis was set at 29 600 km/23 229 km altitude over the Earth's surface (= circular orbit with the respective radius) when

the orbital period is 14 hours. This constellation is meant to be positioned in a Walker 24/3/1 configuration – 24 satellites in 3 orbital planes (Bartolomé et al., 2015).

By April 2023, there were 28 launches of Galileo satellites – four of them during the IOV phase in 2011 and 2012 (GSAT0101-GSAT0104) and twenty-four during the FOC phase (GSAT0201-GSAT0224). As of April 1st, 2023, 4 satellites are not available or usable for the Galileo service – GSAT0104 (unavailable from 2014 until further notice); GSAT0201 + GSAT0202 (unavailable from 2021 until further notice); GSAT0204 (removed from active service in 2017 until further notice) (GSC, n.d.c). There are also several launches planned to complete the FOC phase with operational satellites. This should be operated by the Arianespace company which will substitute Russian contribution during the mission (Arianespace, 2022). Moreover, once the Generation 1 Galileo satellites will be in space, the Generation 2 satellites should come into place and enhance Galileo's capabilities with the first planned launch of G2 satellites for 2024. These satellites are not meant to substitute the existing satellites but exceed the present provided service according to the evolving needs of users. This should be secured by brand new technologies such as more precise atomic clocks, navigation antennae, or security mechanisms to prevent Galileo signals from unauthorised damage (ESA, 2021). The second generation is being developed by Airbus Space Systems company with the aim to meet the developing requirements of navigation system users with expected operability designed for 15 years. In March 2022, the company announced the preparation phase of production of the first six Generation 2 satellites in Friedrichshafen, Germany. ESA, EUSPA and EU agreed on the design of system utilities the Airbus company implemented and developed just before the announcement, which paved the way for the early stages of production, further verification, and qualification of equipment (Airbus, 2022). As per the announcement by Thales Alenia Space (one of the developers of G2 satellites), the new constellation of Generation 2 Galileo satellites should be much more reliable, precise, and mainly cyber-secured which is nowadays one of the biggest threats in the world of developing technologies and the upcoming digital decades. Additionally, the new generation should empower the EU's space industry competitiveness in this definitely strategic domain which is one of the key components for aimed EU sovereignty (Thales Alenia Space, 2021).

ESA has already confirmed that Galileo is nowadays (2023) the most precise satellite navigation system currently operating (ESA, 2023). G2 satellites will revolutionise the

fleet and improve accuracy to decimetre-scale to all the users instead of current metre-scale precision. Even if the new generation satellites will be much larger than the previous ones, the technology will allow launching two satellites at once as today. The biggest 'upgrade' is the fully digital payloads that will allow the Galileo operating personnel to actively respond to the users' needs in time. The increased number of satellites in space will also enhance its performance and downsize the dependency on ground-based centres with increased security for Galileo's signals preventing unauthorized use (eoPortal, 2022).

As space technologies cannot fully control themselves without a human factor, there are necessary ground-based control, monitoring and transmitting centres. Even if the ground segment is not responsible for the navigation and signals itself, its role is crucial in supporting mechanisms which they provide to the Galileo services. Galileo headquarters are based in Prague, Czech Republic, but the core of the ground-based system consists of two Galileo Control Centres (GCCs) in Germany (Oberpfaffenhofen) and Italy (Fucino) Many other smaller centres are scattered all over the globe. The main control centres manage functions with the support of the Ground Control Segment (GCS) and other Ground Mission Segments (GMS). GCS's main function is to handle the maintenance of the satellites and constellation, ensure everything is operating correctly, and verify the safety of the system. On the other hand, GMS is handling the navigation and timing data by means of communication via the Galileo network of satellites and Galileo Uplink Stations (ULS) which distribute the data (GSC, n.d.d).

The Galileo Control Centres are also part of the Ground Mission Segment, which is a worldwide network of ground-based facilities responsible for Galileo operations and functions. There are several other stations such as Ground Sensor Stations (GSSs) which collect and forward Galileo data in real-time to GCC, or already mentioned Mission Uplink Local Stations (ULS). On the other hand, Galileo Control Centres are also part of the Galileo Ground Control Segment together with Telemetry, Tracking & Control Stations (TT&C) which collect telemetry data (Bartolomé, 2015; GSC, n.d.d).

The key role of the control centres in Germany and Italy lies in the collection and distribution of the navigation data to the final users. These two centres serve as some sort of centralised spots of the other supporting centres which run the whole Galileo mission and manage its functions. Their responsibilities are not just ground-based since these two

centres also monitor and control the performance of the constellation in outer space during tests and operations' preparations. Moreover, GCCs are also at the centre of cooperation with external entities which send data to Galileo receivers. Their role is to multiplex the data and messages into a single data stream which can be transmitted to individual stations and further used in the space segment. This is primarily connected with the safety of the technology and data encryptions which lie on the back of the controlling responsibility of these centres as a key for future development and authentication of the service. While all the main services are provided based on online communication and on-time service, GCC's role is to use the long-term perspective for planning and future events scheduling by using and controlling online and offline data streams from past missions or non-operating satellites (Bartolomé et al., 2015).

Finally, there are also Galileo Security Monitoring Centres (GSMC) located in Saint-Germain-en-Laye (France) and San Martín de la Vega (Spain) which oversee monitoring and action-taking in case of external security threats and alerts. Moreover, these centres also monitor the operational status of Galileo components. If an imminent threat to the EU member states will occur in connection with Galileo system usage, EUSPA will then issue instructions approved by Council to GSMC which is responsible for their implementation (EUSPA, 2021a).

As for the G2 satellites, there will also be brand-new ground-based centres and infrastructure which should empower and enhance the performance and security of the system. The key G2 Ground segment will consist of several centres such as:

(1) G2 Ground Control segment (G2GSC) – to control all the G2 satellites;
(2) G2 In Orbit Validation Ground Mission Segment and Secured Facility (G2 GMS-GSF) – to provide new capabilities for users;
(3) G2 In Orbit Validation Security Monitoring (G2 SEC MON) – to monitor all the security measures of the Galileo constellation and system;
(4) G2 System Test Bed (G2STB) – to develop and validate all new Galileo capabilities;
(5) G2 Public Regulated Test Bed (G2 PRSTB) – to develop and validate all new Galileo Public Regulated Service capabilities;

(6) G2 Security Chain Test Bed (G2SC) – to secure full compatibility between security provisions and systems between space segment, ground segment and receivers;
(7) G2 Filling Device (GS FD) – to provide secure communication (cryptography) between different systems of the G2 system (eoPortal, 2022).

As it is clear, the new generation aims for a huge development in the security area of Galileo systems. The focus is predominantly on the provision of safe and secure service which will be resilient to third-party interferences. These provisions also point out the aim of the EU's sovereignty plan in strategic areas such as outer space and ensure its leading position within the positioning, navigation and timing sector. As of nowadays, three billion users are under Galileo service, and all smartphones sold in Europe should use Galileo's receivers. With further development and implementation of the G2 satellites, the number of users should increase manyfold in the individual and commercial spheres (eoPortal, 2022).

1.3 Galileo's position in the global space (satellite) system

There are currently four major global navigation satellite systems and two major regionally limited satellite systems:

(1) GPS (USA)
(2) Galileo (EU)
(3) GLONASS (Russia)
(4) BeiDou (China)
(5) QZSS (Japan) – regionally limited
(6) IRNSS/NavIC (India) – regionally limited

While the first four of them have real global coverage, the last two are regionally limited. Japanese QZSS can be understood as an augmentation constellation enhancing other GNSSs providing much more precise information than a single global coverage constellation would solely perform. On the other hand, there is also a regional system covering just a limited area (Indian IRNSS/NavIC) of the Indian region + 1 500 km around the mainland (GPS.gov, n.d.). In addition to robust QZSS and IRNSS/NavIC, Europe has its own regional augmentation system that makes the service of GNSS more precise in the Europe and North Africa areas – EGNOS (European Geostationary Navigation Overlay Service). This augmentation was deployed mainly to secure the

Safety-of-life services in this highly populated part of the Earth. This promotes straight cooperation between the European Union and other actors with the overlap to the global markets (EUSPA, 2023b). There are also other important augmentation systems focused on GNSSs which help to provide better accuracy in several areas such as Wide Area Augmentation System (North America), Michibiki Satellite Augmentation System (Japan), GPS-aided GEO-Augmented Navigation etc. (EUSPA, 2022a).

It is hard to define which of the global coverage systems is the best since it really depends on the location where the particular evaluator is based. From the point of view of the technical and most precise (accurate) perspective, Galileo is the best (and youngest system to exist. But as mentioned before, for different areas there are pre-set systems providing the positioning, navigation, and timing services to final users with respective accuracy. At the place of the best performance of all the systems, Galileo can provide the most accurate information in comparison to the three other systems based on the advanced technology used in the satellites. Chinese BeiDou is then the closest rival in accuracy since their merits are almost the same numbers-wise, but with far more satellites and less technological stability (De Ingenieur, 2018; Timbrook, 2021; Peng, 2020). Moreover, G2 satellites should bring far more precise data and information to final users than is presently available (Thales Alenia Space, 2021).

2 Threats to Galileo Global Navigation Satellite System

The navigation system is one of the strategic elements of the national, multi-national and global sense of living. Moreover, it is a crucial part of how post-modern society became accustomed to this 'natural' service. What would happen if the navigation or positioning system would suddenly collapse? The aircraft transport would stop, the integrated rescue system would be ineffective, which would lead to numerous human-life losses, and multi-national armed conflicts would return to their roots of strategy Moreover, economies of the world would start to collapse, and financial losses would rise to unimaginable levels. Technology development as it is known nowadays would disappear by this single shutdown of PNT systems. This does not mean that the danger is in destroying the system, but rather also lies in harming or limiting its functions or misusing the service for different purposes which the system is meant to provide.

The harm to the essential navigational systems can be either intentional or unintentional, signal or system interfering, kinetic (physical) or non-kinetic (directed energy), but none of these options are desirable. Any type of interference generally means serious issues for the providers and users of the service. This chapter aims to present, describe and conceptualize the main technical (material) threats to the Galileo Global Navigational System by listing their brief specificities and categorization under intentional/unintentional threats.

Additionally, it is important to mention human failure threats that are not part of any of the below-specified categories, but can easily lead to a propensity of the other types of threats. Human failure threats are simply poor installations performed by the engineers constructing the satellites, which can consequently lead to other system failures. A common example includes bad positioning of the antenna during installation ends up hindering the ability to obtain a clear view of the sky. In this situation, the user cannot rely on a clear signal from the satellite. This is mainly caused by poor product design, obscuration of other parts of the satellite or not taking into consideration the ground development of taller buildings. This results in errors in the location and time information, or at worst a loss of signal (Spirent, 2018).

Second on the list of threats that do not fall neatly into the specified categories is user error. This is mainly caused by users who over-rely on the information provided by the system, instead of critical evaluation of presented facts from other systems and the

surrounding world. User error should be also considered to be a threat to GNSSs since people still play a crucial role in functionality and further development. Moreover, when poor service is presented to the user who relies on the data rather than on holistic evidence, this can lead to wrong decision-making in everyday situations (Spirent, 2018).

2.1 Intentional (man-made) threats

Intentional threats are those when the system is being attacked with the aim to damage it or change the data and service the system provides according to the attacker's interest. There are four key types of intentional attacks towards the GNSS – electronic attacks, cyber-attacks, kinetic (physical) attacks, and directed energy (non-kinetic) attacks.

2.1.1 Electronic attacks

Electronic attacks are one of the most well-known and most experienced in the question of disruption of satellite service provision. Jamming is one of the electronic man-made threats to the functionality of Global Navigation Satellite Systems. As for this element, local radio-frequency interference is used for scaling down the satellite signals, which leads to a loss of signal in the case that the jammer (the device causing the interference) is blocking all the satellite signals. The usage of jammers (so-called "personal privacy devices") is known from usage in company vehicles to inhibit movement tracking (for example during Mexico's truck thefts) (Spirent, 2018). Nowadays, jammers are available to purchase at low costs in nearly every part of the world, and at any size. The interferences made by such devices can be far-reaching threats not only to the signal, but also to interconnected sectors such as the economy or critical infrastructure. Even in this category, the element of jamming can be unintentional because of the different frequencies the GNSS works – for example from medical equipment, cellular communication, or Wi-Fi usage. On the other hand, these are minor interferences causing negligible errors. The simplicity of intentional threat is in the way how the jammer can draw down the signal – as the signal is flowing from the satellite, the intensity is lowered according to the reached distance – then the jammer performs a high radio-frequency activity and thus attenuates the satellite signal, which results in loss of positioning, navigation, and timing service. The main threat is not from small jammer usage, but rather from large-scale jammers which can cause huge economic losses and can be used during military operations such as during the 2011 'frequency war' between North Korea and the U.S. when the Asian country was accused of several usages of jamming which also

affected South Korea (Mukherji and Chandele, 2021). In the opposite of other (kinetic) attacks, once the jammer is turned off or deflected from the satellite's frequency band, the service is restored so the 'damage' is reversible. There are two types of these devices: uplink and downlink jammers. The first category interferes with the signal heading to the satellite from the ground and prevents the satellite operators from sending commands to satellites. On the other hand, the downlink jammer blocks the signal coming to the ground from the satellite and clutters the receiver's end with noise (Harrison et al., 2017).

Spoofing is a slightly different interference to the satellite-transmitted signal, but it still must be considered as an electronic threat to the smooth functioning of GNSS. The effect of a spoofer (device causing spoofing) is based on transmitting or rather broadcasting fake signals to the final user's device, resulting in false location information indicated in the position application. At that time, the device is fooled, and it believes that the information received is correct. For quite some time, this threat was not considered to be a big one since spoofing was extremely hard to perform. However, open-source software and low-cost components have recently changed the situation (Spirent, 2018). Since reliable data and perfect position information have become key components of current technologies, spoofing has become a serious threat to such receivers, especially to unmanned aerial vehicles or drones that rely heavily on exact data. Spoofing occurs when a stronger signal overpowers the GNSS signal from the satellite and influences the radio transmitter to send false information to the final devices. There are known examples of state-sponsored spoofing, such as when a certain state uses spoofers to prevent drones from entering their aerial zone (Lopez and Simsky, 2021). The biggest threat is that the spoofed user/device influenced by the wrong information for a longer period can induce dangerous behaviour of the used platforms which rely on time and location data provided by the GNSS. The spoofer replicates the radio-frequency carrier, and a bit changes the data and code of every GNSS signal which is in the targeted area. Once the meant-to-be-attacked signal occurs, the spoofer sends a similar code of information with a little redesign to overpower the original one and deliver it to the final user. Every signal then has the same spreading code as the true signal but the information in it is changed according to the purpose of the attack. This leads to a loss of reliable data (Psiaki and Humphreys, 2016). There are also two ways to spoof a signal: downlink and uplink. Understandably, the downlink signal influenced by the spoofer will perform badly as described above within the final users' devices. On the other hand, the uplink signals

transmitted to the satellite and affected by the spoofer can cause the satellite to be taken over for unauthorized use (Harrison et al., 2017). Finally, there is also spoofing without changing the code, but just recording the authentic signal. Due to smaller code delay and faster reaching of the signal peak, the final device will lock on earlier to the recorded signal than to the authentic one – this is called meaconing. Once the signal is locked, the receiver stops the search and the spoofed (meaconed) signal starts to produce wrong PNT data when the receiver lets the signal perform tracking (Syam, 2022).

Last but not least is radio frequency interference, which is quite similar to obscuration because it limits the effectiveness of GNSS. The difference lies in how radio frequency interference is presented by different electronic devices which produce noise that obscures the true signal and does not let it go through. Once there is a bunch of radio frequency transmitters, the noise made by them can occur as an object which is limiting the satellite signal to reach the user's device with the information of position and time. The final user then experiences a loss of signal which is blocked out by the noise or severe errors in positioning accuracy. This usually happens near cell towers or within devices which have inappropriately shielded GNSS receivers from other components (Spirent, 2018). Moreover, it is important to mention that even a limited radio frequency signal transmitted near the GNSS true signal partially affects the true signal but with no significant effect on the final user (because of incorporated radio frequency filters) (De Bakker et al., 2006).

2.1.2 Cyber attacks

One of the most famous man-made threats to every technology-based device is hacking, which manipulates the performance of the GNSS by changing the device software directly or attacking it with harmful code which evolves by its implementation. This is mainly observed in the case of mobile devices, as they are easy to attack via a single untrustworthy application which is installed by the user. This software usually attacks the operation system and allows the GNSS signal's receiver to edit the information manually according to the attacker's will. This leads to false position and timing information which the device and user are relying on. This can be problematic mainly because of the huge impact on autonomous devices which are built to be dependent on reliable and precise data (Spirent, 2018). This is also linked to nowadays widely discussed cyber-attacks which can completely cut off the positioning system when the attack is successful. Satellites are not an exception from those devices which are vulnerable to being under

such attacks. When hacking is often associated with influencing the final devices, cyber attacks can be pointed onto satellites, their performance, and contained data. The effect of using them against space systems then ranges from loss of data to complete loss of the satellite via shutting down the communications or damaging the electronic components. At the same time, for the ground-based controller, it does not have to be evident what caused the damage or loss of control. Afterwards, tracking the attackers is quite hard since there are thousands of systems and devices that are able to hide or obfuscate an identity (Harrison et al., 2017). A survey conducted in 2022 revealed that cyber attacks pose the greatest threat to the GNSS data because of their affordability, speed, and difficulty to be tracked. A successful cyber attack against the whole GNSS constellation could collapse economies and bring civilization into chaos. For instance, global financial losses caused by cyber attacks conducted in 2021 were estimated to be 6 trillion USD (Peeters, 2022).

As evidence shows, lower cyber security measures within the space assets significantly promote this type of attack, since it took a long time for policymakers to believe that cyber is an important domain which should be focused on. The number of cyber attacks increases every year, and some case-relative events have already reported – i.e., in 2008, two of NASA's satellites were taken over by Chinese hackers for a couple of minutes. Another important cyber attack against GNSS was recorded in 2018 during NATO's Trident Juncture military manoeuvres when the satellite ground-based systems were disrupted and enhanced the need for mitigation of risks with preventive mechanisms and simplifying necessary controls to avoid neglecting cyber security measures for all systems working together (space or ground-based). Moreover, cyber campaigns and attacks became important factors in Russian foreign policy during operations against their rivals. This approach was also recorded during the beginning of the war in Ukraine in 2022 where the private sector's Starlink satellites were targeted but significantly succeeded to restrain the effect, and no serious impact of the attacks was noticed (Cesari et al., 2021; Pražák, 2022).

2.1.3 Kinetic attacks

On the opposite of remote attacks, there can be also kinetic attacks, which aim to damage the satellite physically. The most typical example of this scenario is to strike the satellite or use a warhead detonation in its vicinity. This threat was well demonstrated in 2007 when China tested positively on its ASAT test and struck down its own satellite. In 2019, India became the fourth nation which succeeded in ASAT testing (Harrison et al., 2017;

Tellis, 2019). This is mainly a threat for satellites in Low Earth Orbit because a higher number of states (actors) are capable of owning or developing weapons to strike satellites at this altitude. On the other hand, the 'space hegemons' have the capability of more complex weapons and missiles to go further into Medium Earth Orbit, where positioning satellites reside. This also brings another factor – the higher the satellite is, the longer it will take for a missile to hit it. For example, the missile meant to strike a satellite in Geosynchronous Earth Orbit usually takes more than four hours to reach its target, which allows the 'defender' a bit of time for reaction. The kinetic physical attack must also be considered from other orbital objects already residing in space since these satellites could be used as weapons to attack different satellites as space mines or just 'kamikaze' satellites controlled from the ground. Moreover, the threat is not just explosive because a satellite in the same orbit can also grab another satellite and de-orbit it. It would end up in unrepairable damage, destruction and loss of function of the de-orbited satellite. On the other hand, de-orbiting is not the only outcome that can occur once the satellites touch each other – attachment to the target satellite can interfere with its operation. According to evidence, all the big players in the space field – Russia, China, India and several European countries are aiming to develop and place in orbit such satellites for their own strategic use (Harrison et al., 2017).

However, satellites in outer space are not the only element in danger of kinetic attacks. Rather than deploy weapons against systems in outer space, it is far easier and less expensive to target the ground-based stations supporting the space technology, as they are highly visible and relatively easy to hit. The attacker does not need to completely destroy the station since there are several ways to damage such centres. On the one hand, the centre can be directly hit by rockets (from long range) or grenades or firearms (from close range), but damage can even be caused when water, electricity or communication supplies are attacked and rendered out of order. The main difference between a space-based system and a ground-based system attack is that the effect against the ground system would not be permanent, since these technologies can be substituted or repaired. Meanwhile, there are not many alternatives in place for if a satellite is hit and destroyed, or de-orbited. The specificity of kinetic attacks lies in their destructiveness to the whole space technology, which furthermore affects the final users with loss of provided service (Harrison et al., 2017).

Kinetic attacks also bring forth a long-discussed question of space debris and the danger it poses to other space systems. This was raised mainly after the 2007 successful ASAT testing by China which destroyed their own satellite but left thousands of pieces of debris orbiting the Earth. Currently, there are millions of pieces of space debris orbiting with an average speed of 22 000 miles per hour. These pieces pose a real threat to all orbiting satellites since at this speed a 1-centimetre piece of space debris can cause damage as a 250 kg object travelling 60 miles per hour on Earth. The real threat is for all the services provided by satellites ranging from communication, business, and security system to GNSS. Collision with these pieces could cause unrepairable damage and loss of the provided service depending on which system would be hit (Global Resilience Institute at Northeastern University, n.d.). About 5000 operational satellites are orbiting the Earth nowadays plus an additional 3000 dead satellites. And the problem is when debris causes a catastrophe (once one or more satellites are destroyed), the number of debris pieces multiplies and the probability of collision increases. ESA estimates that there are over 33 000 space debris pieces bigger than 10 cm, most of them in Low Earth Orbit (Hollinger and Learner, 2022). To make the effect clear, kinetic (physical) attacks are then irreversible, immediate, and the risk of additional unintended damage is high (Harrison et al., 2017).

2.1.4 Directed energy (non-kinetic) attacks

Finally, space systems can also face directed energy attacks such as lasers or efficient microwave systems. The efficiency of these weapons is not primarily visible but can be as disruptive and destructive as the objects that directly physically attack the targeted system. The biggest advantage of these weapons is the time in which the target can be hit (this can happen in seconds) and the caused damage does not have to be evident at first sight. Moreover, the laser does not have to be at a close radius and can be situated practically anywhere, such as on aircrafts, ships, satellites, or the Earth's ground. The basis of the laser's attack is usually overheating the pointed system to disable it from working properly and providing the right service. But even if the attacker does not have a powerful laser at his disposal, the low-energy lasers can also blind the sensors on satellites and influence their operability. In the opposite of physical offensives, the outcome is not evident right after the attack since the targeted object is still the same, but the performance can be limited, with visible results coming later. This also brings up

questions regarding the permanency of the energy weapon's attack, while the aggressor can never be sure how much damage was caused (Harrison et al., 2017).

Ground-based lasers are nowadays on the rise since China and Russia are heavily investing in these anti-satellite weapons. This requires high-quality technology as the laser beam must be precise and sufficiently strong to harm the object thousands of kilometres away. This brings about requirements for technology such as adaptive optics and heavily advanced pointing systems for transmitting the laser beam to its target throughout the atmosphere and its disturbance. China reportedly used laser technology in 2006 when blinding U.S. satellites to limit their operability (Harrison et al., 2017). Satellite images also revealed the construction of a huge laser in Russia built as a weapon for 'electro-optical warfare' which is able to completely blind and damage the satellite sensors. This is quite different from the so-called dazzlers which Russia or China are using for temporarily blinding purposes which are experienced on a daily basis (Tingley, 2022). In addition, when speaking about China, they are in possession of multiple lasers with the capability to target them against satellites and potentially disrupt their service and damage them. The ongoing development of these lasers has enhanced their current capabilities, and therefore the scope of their effects has not yet been mapped (Hayes, 2022).

As mentioned above, the directed energy weapon is also a high-powered microwave which can disrupt and permanently damage a satellite's electronics. This can be accomplished in two ways – the so-called 'front-door' which misuses the satellite's own antenna to enter the system – or the 'back-door', which takes advantage of gaps between electrical connections of the system. The 'front-door' is more direct, but can be easily detected and prevented by advanced security systems. Additionally, it must be conducted from the angle within the view of the antenna. On the other hand, the 'back-door' is quite difficult to achieve because it requires knowledge of the electronics of the targeted satellite. The attacker must then find a weakness in the system and take advantage of it. That being said, the attack can be conducted from any angle of the satellite. It must be considered that the outcome is difficult to foresee, and the damages do not have to be evident on the spot (Harrison et al., 2017).

A widely discussed topic is the usage of nuclear weapons in space, their detonation and the following electromagnetic pulse which would certainly damage the satellite's

electronics heavily. However, the effects of this weapon would endanger and damage all the satellites in the line-of-sight (irrespective of the intended target) and would alter the space environment with additional radioactivity that would affect all the satellites in the targeted orbit (Harrison et al., 2017). Several tests in the atmosphere (up to 400 km above the surface) were conducted in the 1950s and 1960s during the ongoing Cold War with various degrees of success (Fehner and Gosling, 2006). Finally, nuclear weapons usage was prohibited from use in space in 1963 by the Partial Test Ban Treaty signed by over 100 nations (without North Korea or China) (Harrison et al., 2017). In 2022, China conducted an experiment simulation of a nuclear blast in near-space (Mesosphere) which was at an altitude of 80 km from the Earth's ground. At this level, the explosion would be much more harmful than detonation in space itself. This is because of the presence of air that would transmit the radioactivity to a wider area and destroy or heavily damage the satellites in near-Earth orbit. Five minutes after the detonation, the radioactive cloud would rise up to 500 km and affect all the spacecrafts moving in the cloud with strong gamma rays that would trap and practically destroy the satellites in it (Chen, 2022).

2.2 Unintentional (natural) threats

There are four recognized natural – unintentional – threats for the signal transmitting for the Global Navigational Satellite Systems. It should be noted that the physical threat such as collision with space debris must be taken into consideration as a threat to the GNSS, as discussed and mentioned in the previous section. While this should be remembered when considering unintentional threats in the case that the collision of pieces is not intended, it will not be further elaborated upon in this section.

The most obvious signal-harming threats are solar storms, which are electromagnetic interferences caused by solar activity ending up in the loss of signal or occurring errors on users' devices. This heavily affects the accuracy of positioning and location systems in time. This threat is quite predictable, but still cannot be effectively prevented from the point of view of signal protection. These storms negatively affect the service over wide areas in periods of intensive solar activity and flares by drowning out the satellite signals in space (Spirent, 2018). The solar flare affects mainly the ionosphere (from 60 km to 2 000 km altitude) where this extreme space weather characterized by increased solar X-ray and extreme ultraviolet irradiance causes unexpected ionospheric interferences. Therefore, this empowers the noise level and causes the loss of lock of GNSS respective signals which has a major impact on the GNSS's accuracy and service provision. This is

one of the main errors which occur in the mentioned systems causing tens of metres of inaccuracy or full signal loss because of a delay in signal transmission from space to final users (Cheng et al., 2019).

Slightly similar to the previous threat, there is also a scintillation threat which is natural and cannot be prevented. Scintillation is best understood as an irregular ionospheric activity that refracts and weakens the satellite signal transmitted from space to final users. This effect is most often performed in tropical latitudes and at high latitudes (Spirent, 2018). The user is then affected by this phenomenon with lower accuracy of positioning service or absolute impossibility to lock on the signal and calculate the location information during the high intensity of a scintillation event. Usually, this effect is one of the outcomes of irregular solar activity, but is also dependent on geomagnetic activity or lower atmosphere waves which propagate into the ionosphere (Space Weather Prediction Center, n.d.).

The third non-intentionally caused threat is obscuration, which, unlike the former threats, is not caused by space weather. This phenomenon is caused by an insufficient number of satellites, leading to a lack of 'eyes' covering the respective area. This can be experienced when the antenna is blind, and some object is obscuring its view of the sky. Moreover, this effect can also be seen in times of scaled-back operability of the constellation, when there are not as many satellites in view as needed to provide accurate location information to the final receiver. The outcome is then a loss of signal or inaccurate position information for the final user. Places, where this phenomenon is often experienced, are underground or indoor areas, mountain valleys or woods (Spirent, 2018). Obscuration can pose a significant problem to the military, especially when operatives rely upon real-time precise data in areas which are hardly accessible. Even several-floor buildings or dense vegetation can lower the accuracy or end up with a loss of signal for communication and in-time location service. This can then lead to failure in the respective mission or unnecessary damages caused by imprecise data which the leadership or operatives were relying on (Cast Navigation, 2016).

Last but not least of the natural dangers is the multipath threat source. During this phenomenon, the antenna is visible, and the signal is transmitted, but because of some structures/objects near the signal-transmitting path, the information flow can be fragmented on the way to the receiver (Spirent, 2018). The signal is then not simply

received by the user directly from the satellite but is diffracted from the semi-obstructing objects and leads to shifting of the calculated position. Simply put, the longer way the signal must take, the worse the positioning service is provided. As of this, the effect is highly geometry-dependent and usually affects a maximum of up to two satellites when it appears (Kos et al., 2010). This is commonly experienced in urban areas with a high density of tall glass buildings where the signal is fragmented and lowered by the structures, but not lost as in the case of obscuration. The thorny signal path then affects the accuracy of positioning service and errors in location information, but lasts for just a few seconds or minutes (Spirent, 2018). On the other hand, the effect can be experienced for a longer period over a vast calm water surface, since the surface acts like a mirror for the satellite signal (Kos et al., 2010).

3 Operationalization of threats prevention in the case of Galileo GNSS

Current Global Navigation Satellite Systems are in most cases the peak of technological development, which can be reached by the available materials and systems. At the same time, these systems have also strategic meaning for their owners, which must be secured by the best technology accessible. Galileo GNSS is not an exception in this approach since it is under unending development that enhances its strengths and suppresses its weaknesses. The previous part of this diploma thesis presented the most actual and known threats for such space systems as Galileo and what the satellite navigation systems must face once being designed or operated in outer space. Such systems of strategic meaning have their own set mechanisms for how to prevent or defend against the mentioned threats even if they are real (experienced) or hypothetical.

As highlighted before, human failure is a category which does not fit into any of the four intentional categories and is rather a general problem that poses a general threat to any system or service all around the world. Human failure is difficult to prevent, and the only way to secure the best performance is to carefully select the people who will be participating in the project from the service provider's side. The same work must be done to reduce human errors – the achievements must be feasible, the proper tools and materials must be achievable, and development or maintenance plans must be communicated clearly (Ellison, 2018). EUSPA as the agency covering all staff recruitment is offering professional development and training which should secure a good work-life balance and workers' well-being. It claims that they are creating a supportive and healthy environment which should reduce the space for human error. This is also linked to various training and development opportunities which should develop the personal skills of the assignees and help the individuals to become the best in their field of expertise (EUSPA, 2022b).

3.1 Intentional (man-made) threats

Man-made threats presented before are those which are focused on the most since their producers are people, so the attack's mechanism can be prevented more easily than in the natural threats. At the same time, these threats are in some senses more dangerous, since they cannot be predicted in advance for most of the cases. Galileo GNSS response or prevention measures are diversified according to the type of attack.

3.1.1 Electronic attacks

Jamming was presented as one of the most common and cost-achievable options on how to interfere with a satellite signal, which would affect the positioning, navigation, and timing services. The usage of large-scale jammers would then affect not only a few receivers but could cause damage to national security. Since these effects are quite known according to their availability and performance on a smaller scale such as in vehicles, the GNSSs are quite effective in preventing signal interruption on a large scale which would threaten the strategic aims of individual states and economies. Techniques how to mitigate the jamming effect such as changing frequency allocation are quite hard to achieve so only critical sectors are multi-GNSS (switching between GPS and Galileo for civil aviation) and multi-frequency systems used. Cooperation and substitution possibility between GPS and Galileo is crucial for such sectors since without communication between these two, once large jamming attacks occur, there are at least a few minutes of the blind spot of the signal (Mukherji and Chandele, 2021).

For ordinary anti-jamming prevention algorithms or mechanisms, several have been 'invented', but the efficiency differs based on the time of reaction against the jammer. Galileo G2 satellites have been developed to be the best technology achievable with the most complex algorithms, which should prevent possible attacks to be effective against its signal. The length of the code of signal for Galileo satellites is 4092, chips which are almost four times higher than for GPS. This means that the signal is much more complex and stronger, so a more powerful jammer must be used for the whole signal interference. At this point, once jamming occurs, the signal would become less accurate but not unavailable. As for Galileo, the Normalized Least Mean Square (NLMS) algorithm is already used, approved and efficient as a noise adaptive filter. This is an effective way to fully prevent damage caused by jammers. Its biggest advantage is its lower complexity, which allows a quick response to experienced interference. NLMS algorithm, in general, finds the true signal and downsizes the targeted stream to one bulk to minimize the possibility of error. As it is not possible to implement a component that would secure the coming signal from the satellite to receivers, the algorithms must be time efficient. Even if the GNSSs are facing small-scale jamming which is not worthy to be widely discussed or dealt with, the large-scale jamming attack could be mitigated by the NLMS algorithm. In the time of usage of this algorithm, the noise which is on a peak caused by the jammer will drop down under the value which would affect the final receiver. It means that the

service interference will not occur. The advanced technology of Galileo allows NLMS's algorithm usage but such an attack on a large scale which would merit such a solution has currently never been experienced by the system (Dutta et al., 2022).

Spoofing (eventually meaconing) is a bit more intelligent interference which makes the receiver believe that its position is different than actually is. This is achieved by sending false (spoofed) or recorded (meaconed) signals to the final receiver, similar to the original satellite ones. Nowadays a cheap software-defined radio can easily overcome the satellite signal sent to smartphones, so the final receivers work with false data and perform the wrong service. There are several ways how to fight spoofing – once the non-authentic signal is detected, it can be excluded from the bunch of signals which calculate the position. This is not a protection but rather a solution against the occurred attack. Nowadays, receiver's prevention measures are rather detectors of anomalies in the transmitted signal which react to the threat (Simsky, 2019).

Galileo GNSS is using OSNMA (Open Service Navigation Message Authentication) as the anti-spoofing system which is the most advanced available and should secure end-to-end signal transmission from satellite to OSNMA-equipped receivers. The OSNMA component secures the service from unauthorized interference – enabling authentication of navigation data during a spoofing event – and carries the data about satellite location. This is the core service because any data breach or modification would cause a huge inaccuracy in PNT calculation. OSNMA is designed to be a multi-factor authenticator of the signal – it uses hybrid symmetric/asymmetric cryptography which generates a secret key and signature which is consequently added to the data transmitted to the receiver. There is also a public key available to the final devices which cooperate with the secret key and signature and authenticates the trustworthiness of the information received on Earth. If the information is recognized as spoofed, it is excluded from the signal which is used for calculating the position. Since not all the receivers are equipped with the OSNMA component, non-OSNMA receivers are still able to use the information due to a backwards compatible technique. This technique also cooperates with more widely known AIM+ and RAIM+ interference defence systems that are searching for anomalies and comparing them to various satellites' information (GSC, n.d.e; Van Rees, 2021). As for meaconing, since the signal is fully authentic due to being recorded, OSNMA has limited possibilities for detecting meaconed signals. For this situation, the receiver should use its own clock to calculate the delay whether it is as large as the authentic signal should

be and lock to the right one. If the attacker will be aware of this, the time and offset can be set digitally to the accurate length which would confuse the clock but at the same time activate the OSNMA safety measure (Sarto, 2020). Finally, as proved by Curren and Paonni, the length of the encrypted code, advanced multifactor authentication and key sequencing are useful techniques in preventing malicious signals from interrupting GNSS performance. Their analysis of its application and implication proved the signal using the above-mentioned security measures successfully prevented unauthorized use. Moreover, such advanced techniques also provide message/data integrity verification and authentication for all users (Curren and Paonni, 2014).

Radio frequency interference is both – jamming and spoofing. At the same time, it is generally a category of total obscuration of the signal (by an object or different signal) which ends up in a loss of PNT services. Because of the interoperability (in the meaning of the final device's chips) with GPS, the loss of signal due to radio frequency interference would have little or no impact on the user since there would be a switch in the terms of the current provider to the available satellites. At the same time, Galileo relies on monitoring, detecting, and filtering. In certain situations, there are several ways how to mitigate the RFI – for instance, pulse blanking (blanking the incoming signal that exceeds the mean value of the rest of the threshold), zeroing (zeroing the spectral samples above a chosen threshold) or notch filtering (adjusting all the threshold above a certain chosen value). The last mentioned is the most time-consuming and the least effective of the three listed. On the other hand, zeroing and pulse blanking methods both work for different types of interference (Inside GNSS, 2016).

Galileo's high number of satellites which can cover the area simultaneously also helps to prevent interference and object obscuration thanks to the visibility of the respective place by more than just one satellite. This improves the accuracy and lowers the risk of loss of signal due to unintended objects in the transmission way in high-rise cities. This is meant to be the best prevention against natural objects not intentionally targeted against the Galileo service (European Parliament, 2011).

3.1.2 Cyber attacks

Cyber attacks occurred as an essential outcome of development in the information technology field. To fight against these threats, cybersecurity has become one of the hottest topics discussed. Space technology is also touched by this type of threat. Since

humanity is living in a digital age, these types of threats are quite commonplace, and space technologies must be carefully protected to secure a no-problem service provision. The biggest advantages of cyber attacks are their remoteness, cheapness, speed and the hard trackability of the offender. Moreover, it is difficult to defend against cyber attacks due to the ongoing development of the types of attacks. Systems are often left indefensible against new cyber attacks the first time around. This challenges the cyber security officers to answer such attacks almost immediately to prevent any serious harm to the technology. As the development of the attack is still ongoing, the cyber security provisions undergo daily updates to secure their best performance (Peeters, 2022).

As mentioned before, there are two possible types of cyber attacks against GNSS performance – to attack the final user's device or the satellite itself. Since these types of attacks are still against (bigger or smaller) computers, the CIA triad is a main principle of network security. The CIA triad consists of Confidentiality, Integrity, and Availability. Confidentiality impacts privacy and means that the data are delivered only to those who are meant to be delivered to and unauthorized access will be prevented. Integrity indicates the trustworthiness of data during the whole process from the 'sender' to the 'recipient' – transmitted data are consistent and accurate during the whole lifecycle during which they were not changed. Availability then provides the anytime accessibility of the transmitted information to authorized subjects. If one of these components of the principle is not met, it can be labelled as corrupted information or data breach which was probably influenced by a successful cyber attack (Qadir and Quadri, 2016).

On the one hand, there is hacking which affects the user's final device and corrupts the information in there if the cyber-attack is used successfully against the device. For these devices' security, a combination of firewalls, routers, VPNs, analysis tools and security engines should be incorporated to maximize the effect of cyber security against already known threats of attack which would be able to influence the data confidentiality, integrity and availability. If such prevention measures do not comply with the device, the PNT service can perform the wrong service or even can be unavailable depending on the type and purpose of the cyber attack (Sindon, n.d.). Most of the currently available devices (95 %) on the market have some sort of prevention tools available to be bought by the user, but are not pre-installed upon purchase. This has begun to change, and more and more devices are equipped with free antivirus programs or other security software. The market is also full of available free of charge or under a negligible cost additional

software that can defend the device against known threats. However, activating and boosting the security measures are fully the user's decisions since such security programs can read the private and personal data which are in the device (Dawson et al., 2015).

On the other hand, there is also the possibility that the cyber attack will be directly pointed towards the GNSS satellite. The essential prevention measures against such attacks are those pre-installed into the system rather than mitigation scenarios once the attacks occur. This can be concluded only against those attacks and threats that are known and efficient prevention or mitigation precautions are invented. The prevention starts with high-quality and complex encryption of the data streams and software settings. The encryption is not just implemented onto the entry point, but also the data itself is encrypted as well as the communication streams where information is transmitted (Oruc, 2022). Galileo cyber security operations are operated in cooperation with National Cyber and Information Security Agency based in the Czech Republic since the Galileo GNSS headquarters are based in Prague (NCKB, n.d.). Since the representatives of Galileo are highlighting the dependence on space, there are also ongoing updates and enhanced prevention measures in the security area of GNSS. In today's highly competitive age, they see detection tools precautions as the most important to at least mitigate the impact of the possible threat. Moreover, since Galileo is a strategic project on a multi-national level, the quantum encryption level is at the top available to avoid any connectivity corruptness that would lead to the EU's dependence on third-party service providers. EUSPA also combines cooperation between the public and private sectors allowing private companies to contribute to infrastructure security via joint projects of respective algorithms and systems implementation (Gutierrez, 2022). Moreover, the European Union also presented the 7SHIELD project foundation which partly aims to strengthen Galileo's resilience against cyber threats and set crisis scenarios for how to act when such a threat occurs (Gkotsis et al., 2023). As the evidence from Ukraine 2022 presented, the public and private sector partnership can be beneficial in the development of cyber attack resilient technology which would be able to face even state actors' offensive during the cyber campaigns (Pražák, 2022).

As long as cybersecurity threats are changing and developing every day, it is quite hard to set universal security precautions which would avoid any harm from a cyber-attack conducted against GNSS's satellite. In addition, due to the multinational strategic interest, the information on how exactly the satellite systems are secured and what tools or systems

are in their equipment, is private and not publicly available. The fact is that top-level encryption is used together with systems providing the possible detection of incoming and outgoing streams of data and indicating any suspicious activity which could mean danger to the service. Thanks to the number of Galileo's constellation satellites, if such an attack is conducted and detected against one of the satellites, the service provider can be easily transmitted to other available satellites until the attack is averted. The best approach to securing against hacking is to implement the available software precautions to the final users' devices even if they are under a fee charge. The Confidentiality, Integrity and Availability triad is the responsibility not only of the service provider but also of the final user.

3.1.3 Kinetic attacks

Kinetic attacks are those which are the most evident and at this point preventable or defendable due to the physical nature of the damage. On the other hand, the civilization, fortunately, did not face a weaponized conflict which would exceed to outer space but since this is considered one of the new battlefield domains, these threats are not to be excluded. While space-based technology seems to be quite safe from the perspective of direct attack, ground-based technology is much more vulnerable to individual incidents committed by different actors. On the other hand, striking down a satellite is quite a risky step, which would require a military and technology-developed state involved in such an attack. This would probably continuously arise in global conflict (Novelly, 2023).

The only way how to prevent a physical attack against satellites and space-based technology is to hit the rocket faster than it will find its target. Since navigation and satellite programs such as Galileo are highly strategic, defence measures are under heavy development to strengthen Europe's capabilities in terms of resistance against any type of interference. The European Defence Agency then aims to secure the military needs of the domain for Galileo and other strategic projects of the European countries in space (Borell, 2022). While the prevention measures of hitting the heading missile to the satellite would usually place the operators in shortage-of-time decisions, there is a second option – to manoeuvre the satellite out of the missile's direction. This can be understood as a part of the collision avoidance strategies which was already performed by Galileo in 2021 when manoeuvring off the collision course with another space object. While the experienced manoeuvre was planned and there was plenty of time, as a reaction to the imminent missile threat the manoeuvre would not be fully sufficient. On the other hand,

these capabilities are being developed to be able to perform such moves in a shorter time (Cozzens, 2021).

As clearly understandable, the defence systems preventing physical attacks against satellites, or ground-based systems are more military than technology dominant. This would end up in a warfare dilemma which would affect multiple actors and lead the space hegemons into war in the case of a successful attack against each other. On the other hand, ground-based centres are much more vulnerable to a bigger number of actors such as individuals or terrorist groups since it does not require an advanced long-range rocket system (Harrison et al., 2017). At the same time, such as satellites, the centres are strategic military zones with the highest military technology and personnel security which should prevent on-ground attack. With increasing dependency on PNT service, the defence system is also being developed and measures enhanced (Borell, 2022).

The 7SHIELD project not only provides scenarios and provisions for the cyber domain but also addresses fears of physical attacks and enhances security measures. Due to the higher reliance on the PNT services, the intention to fund such a project was vital since any attack against storage, space or ground stations would pose a major safety threat. Hand in hand with enhancing cyber security measures, the physical attacks domain should be also prevented by several passive radars or laser technologies. The project outcomes should then serve as prevention, detection and mitigation of any type of reversible threat. Its main technological and instrumental focus is on ground-based systems whose resilience should be enhanced under the EU's critical infrastructure regulations (European Commission, 2020). So far, the project presented tools similar to risk management that help to evaluate possible threat impact, which would lead to the security enhancement of security measures and the total risk. Once the tool is out of the validation phase, it will allow the operators to activate internal and external stakeholders when an immediate threat will occur, implement pre-incorporated emergency plans and solely run the crisis scenario until the event is over. The so far outcomes of the validation phase demonstrate a deep understanding of risks and existing vulnerabilities which are focused on to be eliminated. The 7SHIELD tools are now able to run the pre-crisis, crisis and post-crisis stages when the physical attack threat is imminent (Gkotsis et al., 2023).

The next stage of space weaponization (for some can be understood as a safety increase, i.e. cleaning outer space from debris) will be once any of the big players will finally reach

the phase of development, which will allow one satellite to grab another satellite and de-orbit it without fatal damage to itself. Since these satellites are already under development, they will most probably be finished in nearly years. This will most probably lead to an armament race once one of the space hegemons announces developmental completion (Harrison et al., 2017).

It is important to also highlight the effect of deterrence, which clearly serves as a security measure against intentional kinetic attacks committed by state actors. As known as a theory of deterrence, one actor discourages another from taking action by presenting the costs and risks which would outweigh the possible benefits for the enemy. A key factor is the credibility of the threat the actors are facing. The best known and also partially applicable for this thesis is nuclear deterrence from the armament race and the active threat of nuclear war during the Cold War. Commercial expansion to space eliminated the U.S. and Russia's dominance of outer space capabilities and forced the actors to make coalitions to enhance security, promote responsible behaviour, or prepare scenarios of how to respond flexibly to an attack. The main point of modern deterrence is to actively communicate the capabilities and partnerships to demonstrate the costs and risks to the possible enemy's intentions (Harrison et al., 2017). Additionally, once the space dominance of the U.S. and Russia vanished, predictable coalitions started to arise. The most apparent is the NATO coalition which primarily shows close ties between the U.S. and the European Union under which control is Galileo. This is also deepened by the strong interoperability between Galileo and GPS. Furthermore, a partnership was also declared between Japan and India against China's capabilities (Moltz, 2011). On the other hand, the most significant space multinational partnership is the International Space Station (ISS) currently operated by NASA (U.S.), ESA (Europe), CSA (Canada), Roscosmos (Russia), and JAXA (Japan). This partnership and cooperation continued even after the war in Ukraine broke out in February 2022 and the participants plan on collaborating at least until 2028 (Kluth, 2023).

Space is definitely recognized as a new flexible domain of deterrence with outreach to other domains such as air, maritime and land. Due to the expansion of the capabilities of individual actors, the possibility of threat clearly shifted also to outer space, which finally created multi-domain deterrence covering all the previously separated ones into complex bulk of domains and factors that would be at risk if one side's outer space environment would be offensively interfered by another. Conversely, the flexible deterrence domain

means the capability to react to inevitable incidents in space by situation-dependent means of response such as in all other war-fighting domains. One key fact of space deterrence is its significant terrestrial aspect since its main capabilities currently serve the operations on Earth. Space-based communications, surveillance, early warning, or navigation are crucial for everyday armed forces' operations. These then ease up the logistics, provides situational awareness, and enhance response time, precision, coordination etc. Space assets are also recognized as drivers of terrestrial deterrence switching from the deterrence of punishment (threat of credible overwhelming counterforce) to the deterrence of denial (denial of any benefits which the potential attacker could gain by the attack) due to their capabilities. Additionally, space-based satellites also provide transparency into the state's inbound actions due to the freedom of satellite overflight over a territory of a potential enemy. All these capabilities complete the deterrence of space assets in combination with other domains (Boyce, 2019; Klein and Boensch, 2020).

From the point of view of kinetic attacks, the most common and known threat nowadays is space debris. Since the number of launches and satellites in outer space steadily grows, the chance of collision with other man-made objects does the same. At this point, the end of operability of smaller or bigger satellites and space devices or in-orbit explosions multiply the number of space debris pieces in orbit and endanger the satellites and all the other objects orbiting the Earth. It is widely known that space debris disposal is necessary and strategies to achieve this are being discussed. The European Space Agency revealed its own plan and guideline for how to mitigate space debris and prevent outer space from becoming overcrowded with dangerous pieces of old, non-functioning or destroyed objects which endanger the operational objects (ESA, n.d.d).

It is important to highlight that the most effective way to reduce space debris in outer space is to prevent in-orbit explosions or collisions. This can be either achieved via passivation of the inoperable space objects or collision avoidance manoeuvres (ESA, n.d.d). Even if there is the Outer Space Treaty from 1967, there is no multilateral moratorium on space debris mitigation or solution for its expansion. In addition, there is also no ban on anti-satellite testing even if this sort of action harms the space environment with the highest number of dangerous pieces from the destroyed satellites (Srour, 2022). In April 2022, there was a unilateral self-imposed ban on using direct-ascent anti-satellite missile tests from the U.S., and they called other nations to join their initiative. By end of

October 2022, six other nations joined the initiative – Canada, New Zealand, Japan, Germany, the United Kingdom and South Korea (Bugos, 2022). On November 1st, 2022, the United Nations First Committee adopted the first multilateral resolution calling for direct-ascent anti-satellite missile testing ban with a huge majority of 154-10-8. This resolution reflects the multinational opinion of the harmfulness of destructive direct-ascent anti-missile testing. As for now, there are 4 'successful states' which are capable of anti-satellite missile testing – the United States, Russia, India and China. Besides the U.S., none of the possessors voted 'Yes' for the resolution (Foye and Hernández, 2022).

The European Space Agency in its guideline highlights the approach of strong compliance during the post-mission period to treat the space environment most sustainably and safely. According to the ESA's conducted study, the debris removal must start as soon as possible since starting later means less effectivity due to the higher density of space debris in orbits. This is also linked to preventive measures such as anti-collision manoeuvres or passivation of inoperable objects which should be applied sufficiently before the cascade collisions with the operational and strategic space technology become to appear regularly. Based on the current volume of space debris increase, this is going to happen within the upcoming decades (ESA, n.d.d).

The satellites and orbital stages operating in the LEO region should re-enter the Earth's atmosphere in 25 years after the mission completeness. For the GEO region, there is no possibility to descend back to LEO and then re-enter the Earth's atmosphere. The only option nowadays is to re-orbit such satellites to the 'graveyard orbit' approximately 300 km above the GEO orbit. This should help to clean the protected orbits with commercial and scientific value. For the satellites providing PNT service such as Galileo, the re-orbiting strategy is also applicable to keep valuable space for satellite replacement (ESA, n.d.d).

The European Space Agency also presented the Clean Space initiative in 2012, where it confirmed its devotion to keep developing technologies and approaches to mitigate space debris. This was also about increasing attention to the environmental impacts of space activities on Earth and in outer space, lowering their negatives and preserving orbits usable for other generations (ESA, n.d.e). The current problem of already orbiting debris around the Earth is recognized by ESA, which stated that active debris removal is also necessary along with future plans for how to sustainably use outer space without harming

it for upcoming generations. Clean Space initiative is a tool to develop technologies to prevent outer space from becoming inhabitable to new space objects (ESA, n.d.g). The anti-satellite tests conducted in recent years again proved a need for a legal framework for establishing the conduct of states in space. According to many opinions, a new treaty must be created to protect the space environment and regulate space activities and space debris. On the other hand, the new treaty is not necessary if technological progress will develop instruments which will help the states run their space activities more sustainably (Srour, 2022).

3.1.4 Directed energy (non-kinetic) attacks

Even if the non-kinetic attacks are usually not seen at the first glance, they are as dangerous as the kinetic ones. Sometimes, the effectiveness of directed energy attacks on the satellites can be a much more strategic and low-cost solution for the attackers if the total destruction of the satellite or any other space object is not the main target but rather some part of the satellite should be put out of order. Kinetic anti-satellite weapons proved themselves useful when the subject of attack should be destroyed. On the other hand, if blinding the satellite or just shutting down the service is enough, non-kinetic means of attack are totally advantageous due to their cost, efficiency and speed. This is not a case of nuclear weapons usage since their effect is fatal and completely undefendable. Directed energy (non-kinetic) attacks are then similar to electronic or cyber attacks, but with more fatal and imminent consequences (Harrison et al., 2017).

One of the previously presented threats is a laser attack which can overheat, harm and temporarily or permanently blind a satellite if targeted precisely in a couple of moments. This can also occur as a standard error so the operational centre cannot confirm whether it is an attack or just system overheating, which shuts down the service provision from the respective satellite. The outcome of whether the attack was successful or not is hard to be recognized by the attacker since only the operator will be able to say whether the system is off or not. At the same time, since satellites are a rather strategic technology, the operating state might not announce the attack against themselves at the first moment since the investigation is often ongoing and the result comes with a delay. There is also a second option of the laser attack outcome different from blinding – dazzling – that causes temporary loss of the satellite sight (Kay, 2022).

Ground-based lasers have the capability to influence the service provision and satellites' operability which are mainly placed in the geostationary orbit. Otherwise, the satellite will sooner or later be out of the laser sight due to its orbiting around the Earth. Galileo's satellite constellation is placed on the MEO so in its case this is applicable (ESA, n.d.f). A larger satellite constellation also has an advantage with a lower possibility of a loss in PNT service, since if one or two satellites are permanently blinded by the extraordinarily strong laser, the service is not lost but just weakened due to the substitutability of the whole constellation. In these cases of temporary visibility of the satellite, the satellite is typically dazzled instead of permanently blinded (Kay, 2022).

It is hard to define how to prevent someone's decision to attack the satellite directly with a laser. It is (so far) not possible to develop a successful prevention measure such as a 'shield' which would somehow mirror the laser attack and safekeep the satellite. The laser beam cannot be stopped until the laser itself is destroyed or the energy source is turned off. In responding to the attack, even if the counter-action is immediate, it will not necessarily be sufficient to save the satellite from damage due to the power the laser would have to have to reach Medium Earth orbit (MEO) satellites. A service such as PNT should not be the first on the list of targeted satellites due to its usefulness for all and not only one country. Additionally, since the Galileo satellites are placed in MEO, the laser would have to be extremely powerful to produce enough powered energy beams to damage or destroy the satellite. Today's laser capabilities are limited to hitting and damaging low-orbit satellites, so Galileo should be safe for this time being. That being said, it is important to continue developing technologies to help to prevent damage caused by a high-energy laser beam since space competitiveness is on the rise, and so are anti-satellite laser weapons (Liu et al., 2020). For now, deterrence seems to be the only way of prevention that is applicable for a state actor who would consider using such a weapon offensively (Harrison et al., 2017).

Similar to the previously mentioned, there are also high-powered microwave weapons that can be used for influencing the satellite's electronics – either disrupting or destroying. Both types of microwave attacks are dangerous for the satellite's functions and service provision. On the opposite the laser attacks, these disruptions are defendable from the point of view of prevention. In the case of the 'front-door', most of the satellites nowadays are equipped with circuits which are designed to detect and block the energy beam entering the system through the satellite's antenna. The second type of disruption is a bit

more sophisticated since the ‘back-door’ high-powered microwave attack misuses gaps and seams between the electrical parts, connections, and shields. This also requires quite advanced knowledge of the particular satellite construction to navigate the attack precisely to the spot. On the other hand, this type can be conducted from any direction, while the ‘front-door’ can be used only directly against the antenna. The possible best prevention method is to carefully design and construct the satellites to eliminate the risk of misusing the imperfections. Similar to laser attacks, the attacker cannot be sure about the damage caused since it can be hard to estimate the range of disruption made (Kay, 2022).

As a final part of the non-kinetic attacks comes nuclear weapon usage in outer space. Unfortunately, there is presently no way to prevent damage from a nuclear explosion close to the space object itself. Even increasing the endurance of the satellites is not an achievable feat in the upcoming decades. Nuclear explosions first release a thermal pulse, then radiation and finally particle emissions (Mowthorpe, 2023). One of the prevention measures can be considered the multilateral Partial Test Ban Treaty concluded in 1963 which banned nuclear weapons usage in outer space. This treaty was signed by all the big space actors such as China, the U.S. and Russia (USSR) (Nuclear Threat Initiative, n.d.). Nuclear weapons are not dangerous only in outer space, but everywhere in near proximity of it use. In GEO, the effect would be the lowest since the orbiting speed is the same as the Earth’s, so the effect of detonation would damage only the targeted satellite and environment approximately 100 km away from the explosion. On the other hand, the usage of a nuclear weapon in lower orbits would cause damage not only to the targeted satellite but also to the whole orbit environment and due to the orbital speed and explosion, the radioactive debris would deorbit. This would send numerous pieces back to Earth which would burn out in the atmosphere, but the radioactivity would damage and influence other objects in the orbit. At the time of the attack, the nuclear missile targeting GEO would take about four or five hours to reach it. The advanced warning systems should be then able to warn the actors sufficiently in advance to develop defensive capability against the missile and its possible effect of destroying the particular object (shooting down in an area of no life or no equipment with limited damages) (Mowthorpe, 2023). Consequently, even if the high-altitude nuclear weapon detonation in GEO would appear, it would be less damage-causing due to the long distances between the spacecraft orbiting at these altitudes. Moreover, the level of radiation in this orbit is higher than in

lower LEO so the impact of detonation radiation spread would vanish in a number of weeks. The effective attack would then require large yields (higher than 10 megatons) to cause notable damage (Condrad et al., 2010).

Finally, as mentioned in the section on kinetic (physical) attacks, nuclear weapons usage is a clear example of deterrence on the ground and in outer space at the same time. Space deterrence was already described and elaborated on before, but since this threat is already in sight from the Cold War, nuclear deterrence should be taken into account even if it is being mentioned in the context of outer space. In the past, deterrence was driven by demonstrated nuclear capabilities and an armament race between the U.S. and the Soviet Union which created the bipolar world. Balance of power and nuclear deterrence prevented the nuclear conflict and might help to not break out a conventional conflict between the superpowers. It is possible to say that for outer space, nuclear deterrence merged with space deterrence, but is still present in the means of its content. The usage of nuclear weapons in outer space would definitely lead to a nuclear weapons-involved conflict between capable actors and their allies, which would redraw the world's geopolitics (Harrison et al., 2017).

3.2 Unintentional (natural) threats

Unintentional threats are those which are hard to prevent, hard to presume and hard to blame somebody for their occurrence. These threats do not become real or cause damage because somebody decided to attack or damage the satellite or any other man-made space object, but rather happen due to natural development. As it was said, these are threats made by different natural space objects near the satellite obscuring and influencing the way of signal, or unpredictable space weather.

Solar storms are one of the most well-known and also biggest threats to satellites and their signals. Once a steady number of particles is released by the Sun into space (called a solar wind), these particles come through a solar magnetic field. If the particles are sufficiently strong and ‘shot’ into a particular direction of Earth, eruptions and solar wind become a geomagnetic storm that endangers all the orbiting objects. The Earth has its own magnetic shield that lowers the intensity of the storm and the speed of particles heading towards Earth – the magnetosphere. As such, most of the energy is absorbed and not let further. But if the storm wind is sufficiently strong, the rest of the energy is redirected into the atmosphere near the poles Aurora events are visible. At this point, the space assets are in

danger. The energy beam can then either destroy satellites laying in the thermosphere (including LEO) or heavily affect the PNT service by obstructing the signal heading to the Earth and changing the radio waves travelling through it. This then ends up in significant service inaccuracies. The prevention measures are shielding the satellites or other space assets with advanced materials which can face geomagnetic storms via their resistance against radioactive waves. The second part of prevention is an accurate space weather forecast which would allow the operators to protect key electronics in the satellites, which are the most predisposed to get damaged by geomagnetic and radioactive waves. At the same time, the development can also allow the operators to move the satellites from the way of the wave to limit the possible damage (as was already experienced). Even if the forecasts are heavily developing nowadays, it is still quite hard to predict precisely when and whether the solar storm will occur, as well as if it will be sufficiently strong to get through the magnetosphere (Mehta, 2022). ESA has its own Space Weather Service Network with Coordination Centre in Belgium, which provides high-quality space weather observations and models. This service is under ongoing development and continuously published data are giving more precise information. This information is then used by governments and research institutions to help build the desired Space Weather Service provision system which would be a responsible and reliable source of weather data from outer space. The development now targets improving the data accuracy, which should be then provided to the end-users (private and public sector). The service is currently focused on solar weather, space radiation, ionospheric weather, geomagnetic conditions and heliospheric weather (SWE, n.d.).

Nowadays, the PNT service which is provided to the general public and for business purposes is mostly PPP – precise point positioning – which provides extremely highly accurate positioning data. This can be interfered with and influenced when so-called scintillation occurs. It mostly occurs in the Earth's ionosphere and ends up downgrading the accuracy and strength of the propagated satellite signal. This happens especially often in tropical latitudes and equatorial areas where solar and geomagnetic activities are strongest. Although it seems to be a limited problem, in the time of the strongest scintillation effect, the signal can be completely lost – mainly in the post-sunset period (Vadakke Veettil et al., 2020). While the observations conducted between GPS, GLONASS and Galileo concluded that the scintillation is the strongest for the E5a band, which is Galileo's, the effect is not that damaging. Therefore, even if Galileo should have

theoretically performed the worst during these events from the three above-listed systems, the observation results revealed that the actual most affected service-providing signal is in the case of GLONASS. At this point, it is important to highlight that even if Galileo can mitigate the strength of scintillation, it is still being affected by its effect and thus the performance of PNT can be delayed or less accurate than during 'ordinary' events (Hlubek et al., 2014). The biggest advantage of Galileo GNSS against such phenomena is the constellation robustness which secures the visibility of at least three satellites at the same time, and which partially compensates for the affected signal streams. The constellation was designed to mitigate the effect of variations in total electron content (TOC), which is the ionospheric event part of. In addition, Galileo's service was planned and provided in real-time to secure the safety-of-life service in every part of the world in different environmental conditions. It was revealed that one of the key components designed for avowing the scintillation effect is the ground station receiver's complexity and algorithms that allow signal tracking and raw data operationalization. All the above highlighted is at a high level in Galileo's case which presents the best anti-scintillation effect GNSS available (Lannelongue et al., 2008).

Obscuration, another natural threat, affects the PNT service due to the insufficiency of a number of visible satellites in hardly accessible areas. The signal streamed to the receiver is obscured by a different object, which does not allow the signal to go through it and the receiver is blinded altogether. If the phenomenon extends for a longer period of time, it could lead to a potential loss of PHN service. The best solution for this effect lies with prevention via the size of a constellation. Cooperating satellites can substitute each other in the provision of services and minimize the effect of obscuration (Spirent, 2018). In the case of Galileo, the robustness of its constellation presents the biggest available coverage with at least three satellites in view of the targeted area at the same time. This is the best prevention measure for keeping up the signal alive even in urban areas with a high density of sky-tall buildings or obscuring objects in the direction of signal streams (EUSPA, 2021b).

The last of the listed natural threats is the multipath threat source which fragments the signal transmitted from the satellite to the receiver, which ends up lowering the reliability of the PNT service provided by any of the GNSS. Multipath is difficult to solve in terms of inventing useful prevention measures (Karaim et al., 2018). The best way to enhance the strength of the signal on which the effect of multipath would be limited is the

robustness of the constellation which Galileo is capable of (EUSPA, 2021b). Since it seems to be the most obvious, the best prevention used is to place the receiver into a reflection-free area where the signal cannot be distracted by any of the partially obscuring objects. Nowadays, receivers are designed to use information from more than one antenna (antenna array) to prevent exactly this threat of multipath due to the high-density population in urban areas where this effect occurs. At the same time, the PNT service is also a key component of life in such areas, so the effect must be mitigated by every available source. Once the antenna array technology is used, the receiver can use only the information from the line-on-sight signal which provides the clearest view and signal streamed directly from the satellite. All the other echoes (replicas of the signal) are blocked so they cannot confuse the receiver into bad positioning information (Karaim et al., 2018). It is observed that increased robustness and ongoing development of technology help Galileo to mitigate the multipath threat. Galileo code and signal are more resistant to multipath than other global navigation satellite systems and its performance during these situations is more precise than others. With the increasing number of Galileo satellites and G2 satellites going live, the performance should even improve. Moreover, the receiver's capabilities can strengthen the positive effect of development due to the possibility of using different satellites in different situations according to the actual need (Prochniewicz and Grzymala, 2021).

3.3 Evaluation of the sufficiency of the prevention measures

The previous sections presented the Galileo Global Navigation Satellite System general threats to objects and satellites in outer space, and specifically how Galileo is dealing with them. This section will evaluate whether the current prevention measures are sufficient. The outer space objects, mainly those with a strategic value, can be targets of intentional or unintentional threats, which can influence their service provision back on Earth. To prevent such harm, space and technology engineers are developing prevention measures to secure the longevity and durability of the critical service provider's technology such as PNT satellites. In this part, it is important to highlight which of the presented threats are real and already experienced, instead of those which are on a theoretical basis.

First, it is important to highlight that the EU representatives and officials are aware of the security implications of today's world, and they tend to enhance their safety and security capabilities even if the threat might be just theoretical. Due to high dependency on PNT services, Galileo is considered a critical infrastructure system. Therefore, high importance

is placed on the ongoing development of new techniques and technologies to achieve and maintain a high level of security. New developments to safety measures implemented with Galileo also augment other EU space programs such as EGNOS or Copernicus (EUSPA, 2019).

Electronic attacks are a real and frequent threat to satellite constellations. Since there currently does not exist anti-jamming technology which would fully protect the satellite service, Galileo has already implemented the best available technology: the Normalized Least Mean Square (NLMS) algorithm, which prevents damage to the satellite itself and filters the true signal to restrain the targeted stream. Even if Galileo has yet to experience a large-scale attack, it is good to know that such a prevention system is ready to be used as a protective measure. In addition, G2 satellites will use a much longer length of code that should be strong enough to prevent most of the smaller jammers and keep the PNT service active even during large jammers' attacks (Dutta et al., 2022). As there have been no reports of a serious breach to the Galileo service by jamming, the prevention measures undertaken so far on Galileo can be labelled as sufficient. This serves in direct contrast to the U.S. GPS, which faces continuous attacks due to its age and worldwide usage (Parkinson, 2022).

Spoofing with false signal against Galileo is prevented by OSNMA, which is the most advanced system available and secures unauthorized access to data through multi-factor authentication of the signal via key and signature. Since not all receivers are equipped with OSNMA components, such receivers are not so well secured, and spoofing can occur. On the other hand, all the strategic value receivers that are largely dependent on precise PNT information are equipped with this component since they cannot afford to be easily spoofed. It should be noted that OSNMA has a limited impact on the meaconing threat due to its recorded authenticity of the signal. The only way to counteract meaconing is by having the clock of the receiver correctly calculate the delay. The attacker, who is aware of the length of delay calculating, will then have to digitally change the offset to confuse the in-built clock, which subsequently will activate by OSNMA recognizing an already false signal (Sarto, 2020). The good thing is that even if some receivers are not equipped with OSNMA, they can still receive the signal and information from Galileo satellites due to the backward compatibility. Additional systems also help to search for anomalies in signal transmission and indicate them (GSC, n.d.e; Van Rees, 2021). At this point, Galileo seems to be well equipped against spoofing together with its constellation

size, which also helps to redirect the attacked signal beams to not confuse the receiver. As in the previous section, GPS is facing far more cases of spoofing than Galileo due to the aforementioned reasons. In addition, Galileo has endured large-scale spoofing due to the technology and algorithms used (Fernandez-Hernandez et al., 2023; Parkinson, 2022). GNSS and especially Galileo and GPS are resistant to electronic attacks thanks to their interoperability and easy switch of the PNT provider in real-time for the regular user. This cannot be easily used in cases of strategic systems that rely on pre-defined PNT systems. Galileo has a huge network which ensures the monitoring, detection and filtering of interfered signal beams which applies generally to radio frequency interferences (Inside GNSS, 2016).

Cyber security is a hot topic and as such, it is hard to say if the prevention measures are sufficient in this field or not because the threat and attack development is still ongoing. This type of interruption to the satellites and PNT service providers is very hard to prevent fully, or at least face equally to the threats. Security development is always late since the example of the threat/attack must be experienced first and then the solution for its prevention is invented. In this type, it is rather important for mitigation of the effects with the implementation of prevention measures which will defend the system from any possible future attack, or shorten the response time to a minimum to prevent any serious damage (Peeters, 2022). Galileo's cyber security prevention measures are on the top level among those available with advanced encryption, multi-factor authentication, and screening and monitoring tools. Unfortunately, the final devices are not so well protected since it is not mandatory to have pre-installed anti-virus programmes encrypted access to the equipment. At this point, the PNT service and data contained in the devices and satellites are still in danger and the current situation of the ongoing increase in the number of cyber attacks against GNSS systems just proves the crucial need to secure the cyber domain even in outer space. With a strictly defined CIA triad which characterizes data safeness, the whole end-to-end process must be secured equally with minimalization of possible points of a data breach or system interruption which could negatively influence the PNT service provision and its reliability for critical infrastructure and all the users (Dawson et al., 2015; Gutierrez, 2022; Sindon, n.d.). The ongoing effort to strengthen the systems with cyber security updates is evident since even if Galileo's strategic meaning, the system is updated regularly to provide the highest security level. On the other hand, during these events, the PNT service precision is downsized by the outage of stations

responsible for control and monitoring systems when being updated (Gurzu and Posaner, 2019). The 7SHIELD project is also focused on enhancing cyber security capabilities as well as an automatized reaction system which would evaluate the threat or attack. Based on the results, when facing a crisis, the system would consider all risks and the best approach to managing the crisis, taking into account all aspects of the pre-crisis and post-crisis period (Gkotsis, 2023).

The kinetic type of attack has yet to be experienced in terms of deliberate action by an opposing state. Presently, the only recorded kinetic attacks have been ones used against a state's own satellites or objects in space. However, the European Defense Agency is still developing strategy and prevention measures to secure outer space as an additional domain where an armed conflict can arise. Galileo GNSS would then be the key component of European equipment, crucial for the PNT services which are necessary in military operations (Borell, 2022). For now, the threat remains unrealized, as the point of no return has not yet been passed. The point of no return was first mentioned during the United Nations First Committee meeting, as the militarization of outer space could disrupt the fragile stability between the world (and space) hegemons such as Russia, the United States, European Union, and China. The threat of conflict could arise from an innocent collision between two artificial space objects, and placing blame on the new dual-use technologies combining civilian and military would serve as a detonator of massive conflict leading to enormous economic losses. The biggest backup for peaceful space activities and attack-free environments is international law and the Outer Space Treaty setting rules of responsible behaviour in outer space. Unfortunately, not all states are signatories of the treaty, and a real attack cannot be stopped by international law if the respective actor decides to act illegally. Ongoing development of advanced technologies such as satellites able to grab different satellites and de-orbit them can be exactly the detonator of the armament race and empower thoughts of defence and offence capabilities (United Nations, 2022). Additionally, the 7SHIELD project presents risk and crisis management measures with incorporated reaction mechanisms that should address possible physical attacks. This project's tools are in a validation process nowadays (2023) and their performance is being evaluated on the concrete threats simulated to the system. Based on the outcomes, both physical and cyber security of Galileo's space and ground segment assets should be greatly enhanced in order to endure external threats. As such,

this is a useful enhancement of the currently active measures which should help to secure this infrastructure in the future (Gkotsis, 2023).

Space debris policy is one of the key parts of present-day discussions over outer space and the security of objects placed there. Galileo operators and ESA revealed the Clean Space initiative as a guideline on how to deal with the spread of space debris orbiting around the Earth such as environment-friendly behaviour excluding ASAT testing and self-return of future satellites and other objects that will end their operational life. Unfortunately, the guideline does not include provisions regarding the current space debris, which should also be dealt with via separate cooperation programs with the private and public sectors. ESA is focusing more on future sustainability rather than the current situation solution, including usage of the 'graveyard orbit' that would serve the space objects that finished their mission and are not able to reach back to the Earth (ESA, n.d.d.). As for the public-private sector partnership, ESA mandated Swiss start-up *ClearSpace SA* for the ClearSpace-1 debris removal mission as a first of its kind in 2020 with the aim to remove ESA's derelict part of the rocket launched in 2013 by robotic arms. The launch is planned for 2026 and this mission's possible success can be understood as an approach to how to act towards the out-of-order or not-usable space objects which should be removed from orbits back to Earth (ESA, n.d.h). Moreover, the anti-satellite missiles total ban agreement would be helpful in the run for lowering the space debris orbiting the Earth. Unfortunately, the space hegemons as per the voting for the United Nations resolution are not inclined (except for the U.S. and EU states) to accept such limitation to their strategic development and possible advantage over different actors. This is also linked to the missing international code of conduct for responsible and sustainable behaviour in outer space. Additional regulation can only have a positive impact but to be efficient, most of the space hegemons would have to agree to act according to it. EUSPA, ESA and the EU are actively participating in such framework building and edification, but the real prevention of space debris, its reduction or multi-national agreement is still missing (Foye and Hernández, 2022; Srour, 2022).

On the other hand, non-kinetic attacks are those that are already experienced and must be taken into consideration as threats to be prevented. Unfortunately, technology has not yet advanced to the point that some sort of shield-restraining laser attack would be available. In addition, overheating can also happen even without a laser attack. The prevention shield would have to be manually conducted, otherwise the view would be blocked and

the signal strength would be limited. It is important to mention that laser attacks could take the form of a simple overheating of the system, which would require the attack to be confirmed before implementing any type of shield. At the same time, any shield would limit the PNT service so its prevention measure would be more damage mitigation rather than service provision securing (Liu et al., 2020). On the other hand, if dazzling appears and the satellite is blinded, the shield could be easily used in the direction of the laser beam to restrain its effect. Galileo's prevention against this threat is its constellation size, as even if one of the satellites is blinded, another one in sight can substitute the service and maintain PNT data accurately. Finally, Galileo's satellites are placed in MEO, which would require a high-powered laser to get the dangerous beam to it and damage its function. Such a laser has yet to be created. Therefore, based on the current technology accessibility and approach taken, Galileo is sufficiently secured (Kay, 2022).

In terms of high-powered weapons, the precise construction should prevent the 'back-door' interruption and monitoring circuits can detect and block the energy beams that are calculated to be unexpected or harmful. Any anomalies are then restrained and thoroughly investigated. These are the best options available and quite sufficient for this type of uncommon threat (Kay, 2022).

The most theoretical non-kinetic attack is the nuclear weapon used in outer space (tests were conducted in the atmosphere). This is totally unpreventable without any additional damages. The radiation released by an explosion is destructive to all the surroundings. The globally used prevention measures are firstly legally enshrined in PTBT which bans nuclear weapons in outer space and later agreements. Unfortunately, since these are 'just' agreements, they still cannot effectively stop any capable actor from using such weapons in outer space. Only the additional subsidiary warning systems would allow the other actors to act against shot nuclear missiles, but would never end up with no consequences and damages. This is not a question for ESA, EUSPA or Galileo constellation operators to prevent such attack's possible damages, this is rather a need for a multilateral agreement on how to prevent such attacks from happening (in addition to PTBT and later legislation) (Mowthorpe, 2023).

In addition to the agreements above, it is important to highlight another impalpable instrument – nuclear and space deterrence. This must be understood not only in the view of the EU but rather NATO and generally allies' capabilities. As described before,

deterrence presents costs and risks to the possible enemy, mainly demonstrating that direct attack would not be beneficial. The key role in such theory plays demonstrations of power and capabilities which are able to endanger or deter the counter-actor in case of a possible breakout of a conflict. This applies solely to nuclear deterrence already known from the Cold War, but could prove to be effective in multi-domain deterrence, including the domain of space. One of the space deterrence examples can be the 2007 ASAT test conducted by China against its own satellite to demonstrate its capabilities. Furthermore, all four space hegemons (China, India, Russia, U.S.) were able to perform such a test to *communicate* the *credibility* of their *capabilities* (3C deterrence principles). While outer space is not expected to become a war-fighting domain in the near years, the deterrence concept is definitely applicable here and augmented over allies (the U.S. is a part of NATO where most EU countries are members so the potential conflict against one of the members would involve EU + NATO members). Moreover, even if NATO is not in a position of owning any of the GNSS satellites, they promote sustainable and responsible behaviour towards the space assets by urging to make a legal background for the usage of space-based communication streams with retribution for violation (Boyce, 2019; Cesari et al., 2021).

Fully-sufficient prevention measures for natural threats are much more difficult to develop. That being said, space technology continually undergoes development in order to better predict possible occurrences and mitigate damage or interruptions. Europe has its own system under development, which should be able to precisely predict and evaluate space weather conditions and anomalies once the Space Weather Service provision is completed. Nowadays, the network is providing useful data which is later elaborated by the research institutions, but the forecast system is not perfect yet. The ongoing development should continuously increase its information precision and become far more reliable as time goes on (SWE, n.d.). Presently, space weather anomalies are dealt with by building the satellites to be more resistant to radioactive waves and geomagnetic storms. The improving forecast should also serve the purpose of manoeuvring the satellites when any solar storm is about to occur (Mehta, 2022). Galileo's constellation robustness also helps against phenomena such as scintillation, obscuration, or multipath threat source. The permanent visibility of at least three satellites at the same time ensures that even if one of the satellite's signals is interfered with by one of the previously mentioned effects, there are still others which can act as a replacement. The accuracy of

the provided PNT service could decrease, but this would not affect the regular user. In addition, the complexity of the algorithms and ground receivers which can work with the raw data and operationalize them is advantageous in such situations and helps to avoid the strong effect of scintillation due to its usefulness during safety-of-life situations for which Galileo service is also designed (Lannelongue et al., 2008).

In the case of obscuration, the constellation size is also beneficial since it is highly unlikely that all the satellites in sight would be obscured by some object which would not let the signal through. With the upcoming G2 satellites, their increasing number and their mutual substitutability with the U.S. GPS, the obscuration effect should be experienced less (EUSPA, 2021b).

Finally, the multipath threat source is limited by using information from multiple sources at the same time. This is experienced mainly in urban areas where the signal can be fragmented due to many reflective surfaces. The antenna array then collects data from more than one satellite to calculate the correct PNT data for the user (receiver). As for this technology, most of the reliable data is used from the line-on-sight signal from the clearest view with a minimum of fragmenting surfaces (Karaim et al., 2018). Galileo is also using more complex code and algorithms, so it is much harder to multipath the signal beams thanks to its resistance against echo making (Prochniewicz and Grzymala, 2021). Galileo is thereby dealing sufficiently with both natural effects of scintillation, obscuration and even multipath threat source mainly because of the number of operating satellites which prevent any serious harm to the PNT service provision. Moreover, the increased number of G2 satellites planned for the future will even enhance the durability against such signal-interfering effects.

Electronic threats	Prevention possibilities	Galileo's solutions
Jamming	Changing frequencies, GNSS interoperability allowing their switch in use of service	Length of signal code, complexity of algorithm (NLMS), GPS interoperability
Spoofing	Detection and spoofed signal exclusion from data provision	OSNMA, data multi-factor authentication, AIM+, RAIM+
Radiofrequency interference (RFI)	GNSS interoperability and substitutability	GPS interoperability and substitutability, constellation size

Table 1: Electronic threats, presented prevention measures, presented Galileo's solutions.

Cyber threats	Prevention possibilities	Galileo's solutions
Hacking	Combination of VPNs, firewalls, and security tools to final device	Security tools are available to 95 % of devices, under voluntary use/purchase
Cyber attacks	Advanced encryption, algorithms, mitigation scenarios	Advanced encryption, algorithms, 7SHIELD

Table 2: Cyber threats, presented prevention measures, presented Galileo's solutions.

Kinetic threats	Prevention possibilities	Galileo's solutions
Anti-satellite missile/suicide collision	Space deterrence, international agreements, satellite manoeuvres,	Space deterrence, international agreements, satellite manoeuvres, 7SHIELD
Ground-based system attack	Space deterrence, international agreements, critical infrastructure security measures	Space deterrence, international agreements, critical infrastructure security measures, 7SHIELD
Space debris	International agreements, active debris removal initiatives	International agreements, Clean Space initiative, Clearspace-1 mission

Table 3: Kinetic threats, presented prevention measures, presented Galileo's solutions.

Directed energy threats	Prevention possibilities	Galileo's solutions
Lasers	Deterrence	Deterrence
High-powered microwave	Detection circuits	Detection circuits
Nuclear weapons	International agreements, nuclear deterrence	International agreements, nuclear deterrence

Table 4: Directed energy (non-kinetic) threats, presented prevention measures, presented Galileo's solutions.

Natural threats	Prevention possibilities	Galileo's solutions
Solar storms	Precise forecast, shielding	SWE forecast
Scintillation	Constellation size, complex algorithms, ground station's receivers	Constellation size, complex algorithms, ground station's receivers
Obscuration	Constellation size	Constellation size
Multipath threat source	Constellation size	Constellation size, antenna array

Table 5: Natural threats, presented prevention measures, presented Galileo's solutions.

Recommendations

Global Navigation Satellite Systems are part of critical infrastructure, which plays an important role in a wide range of applications, from aviation and transportation to telecommunication and navigation. For the regular user, the PNT services are something commonly available and a few-minutes loss of signal is not a problem. The important issue is for the globally driven services mentioned above, where a loss of signal, position or correct timing can lead to a catastrophe or huge economic losses. As for Galileo GNSS, this thesis examined the strengths and weaknesses of the system through a detailed description of the danger and how Galileo deals with it. According to it, three identified fields were chosen to be underestimated or not sufficiently secured against interruptions or possible upcoming development in such threats. As for these recommendations, cyber security was chosen as the key phenomenon of a new domain of warfare, its never-ending development and mainly its speed, low costs, and effectiveness. The second underestimated threat is well-known and nowadays discussed as space debris, which is an indirect threat for all space objects orbiting the Earth. The number of uncontrolled particulars in outer space is continuously increasing and no effective method of its mitigation or even removal was tested. Even if Galileo satellites are not in the most utilized orbits, the distance is far, and it is not possible to prevent debris collision by reaching it on time. The only way is to make a manoeuvre, but this can also be a slow action and not sufficient. Space debris as an underestimated threat is listed due to the European Union's multinational effort to cultivate the space environment, but the ESA's presented plan is very vague in its actions. Finally, the last one is the nuclear weapons category in which the damage would be unimaginable. Still, the threat is real, and no particular efforts have been made to make it at least a bit less probable. One of the hard-to-prevent threats is the high-powered laser where there is no effective prevention measure than deterrence or mitigation measures as destroying the laser itself. This threat was not indicated as a part of those underestimated because of three particular reasons – there are no known examples of high-powered lasers that would be able to reach MEO nowadays and threaten Galileo satellites; the power that would have to feed the laser would have to be so enormous that even for the space hegemons it would be difficult to achieve such a level of concentrated energy; and there are presently ongoing development of shielding materials that would at least mitigate the effects of lasers against space

objects. The threat is perceived as a risk and so the approach to developing a defence solution is in the right direction.

As such, it is crucial to ensure the cyber security of GNSS to prevent attacks which could cause severe disruption and damage. It was already mentioned in the previous section that Galileo has the top-level available cyber security measures to prevent any possible, known and already experienced threat tending to interfere with the system. Additionally, even if it is hard to prevent, it should also reflect the possible coming cyber threats to at least harden the hacker's effort to disrupt the system and service. From the point of view of the service provider, it is crucial to implement:

(1) Advanced multi-factor authentication;

Galileo is currently using this type of security measure to generally secure the cyber security triad and data correctness. The more advanced the attacks are, the more advanced the multi-factor authentication should be as well. It would require the users accessing the system interface to provide multiple forms of identification such as passwords (with prescribed numbers and types of symbols) and the biometric scan which would allow access only to those who are authorized to do so. The current multi-factor authentication measures are for hackers weak (password & secret code, authentication apps, authentication calls etc.) for such a critical infrastructure system. By requiring multiple factors including biometric information, it becomes much more difficult for hackers to gain access to the system.

(2) Advanced encryption in-building into final devices;

As in the previous paragraph, this is also part of Galileo's current equipment on how to face hackers and unwanted interruptions. Encryption of the signal also helps to mitigate electronic attacks and minimalizes the PNT interruptions in such cases when spoofing and jamming occur. Algorithmic encryption of the signal is crucial for all three transmitting devices – satellites, ground stations and final users' devices. With the coming options on how to influence the signal from the bottom (final users' devices), advanced should be implemented signal encryption into the final devices which use the PNT data with in-built anti-virus programs which would at least maximise the defence against efforts to corrupt the information.

(3) Conduct regular security audits;

Since the field of cyber security is under a never-ending development, it is important to run regular security audits within GNSS to reveal and identify any vulnerabilities and weaknesses which could be exploited and misused by hackers. Additionally, ethical hacking should be implemented on a daily basis to ensure that even if the threat is known, the system is ready enough to face it without any data corruption.

(4) Increase awareness and training.

It was mentioned many times that the cyber security field is on the rise, so training how to act in the cyber environment safely should be too. All the users of GNSS (operators, engineers and final users) should be trained on how to identify and report suspicious activity, and on the importance of strong passwords and other security best practices. Engineers working with the strategic systems should also pass the security clearance.

As for the second recommendation, there is a space debris ongoing problem. ESA's mentioned guideline is looking a bit ahead and reveals plans for future space debris mitigation, mainly how to ensure that no more debris will be added to the orbits. The issue with the current space debris is being discussed with the private sector and the first mission for a single-piece removal is already confirmed. Unfortunately, the presented solutions do not address any specific way how to at least reduce the orbiting number of particles from the previous decades. Space debris is a big concern for satellites and other space objects' safety.

(1) Active debris removal;

Space debris is not an upcoming problem, it is already a big issue and several collisions have been recorded. With the increasing number of launches and space missions, the threat of a collision steadily increases. Active debris removal should help to keep the space environment 'habitable' by further launches and space objects. In addition, it would decrease the chance of collision and unwanted loss of a particular system, which would end up in great losses in terms of costs and years of development. In the worst case, it could end up in loss of the system's service provision with further consequences. ADR would involve the physical removal of space debris by spacecraft equipped with mechanic arms, nets and other 'cleaning' equipment which would be able to collect or shift the particles out of orbit. ESA should then involve the private sector to conduct the space

debris removal or promote multi-national cooperation in such an effort. The cooperation should be then mainly run by the space hegemons such as the U.S., EU, Russia, China or India.

(2) Laser ablation usage;

The laser was earlier presented as a threat but being used in the right way, it could also be beneficial for space debris removal. This would involve a high-powered laser to vaporize the surface layer of the debris. Consequently, debris would lose its momentum and slow down which would cause the re-entry into Earth's atmosphere and burn up upon the re-entry (Shuangyan et al., 2014).

(3) International regulations.

One way how to reduce the future increasing number of space debris is a multilateral agreement between all the main space hegemons to limit their activities creating free particles which then endanger other space objects, or at least to act responsibly in their own activities with regulations that would secure a safe space environment with minimizing space debris creation (such as the ESA's guideline states). The United Nations is already working on resolution recommendations and general guidelines on how to behave responsibly, but a positive outcome can only come when all the main actors agree on fulfilling their responsibility for future generations.

The last of the recommendations is for the nuclear weapons threat to space objects and missions. Even if this threat was not (yet) experienced, the regulation is old, and no effective prevention measure is available. At this point, the discussion regarding a multilateral agreement would not only tie the signatory states to keep their word but would also sketch the sanction and reaction schemes of the other states. Common sense says that the usage of nuclear weapons in outer space is inevitable but still, there should be established global prevention measures such as monitoring and alerting systems that would warn all participants during such an event. In such an environment, international treaties, cooperation and arms control measures would be evitable. The diplomatic effort is the only way how to act in case of security against nuclear weapons and their effect mitigation. In an ideal world, transparency in space activities would make outer space much safer space than any other concluded agreement.

Overall, the combination of these recommendations should make the outer space environment, GNSS technology, and PNT service much safer and sustainable. Even if some of them are not realizable in a short period, it is important to keep them in mind as an alternative or possible solution for the presented threats which seem to be underestimated by Galileo (and potentially other GNSS systems).

Conclusion

The presented thesis was elaborating upon Galileo GNSS, possible threats to its service and functions, and its solutions on how to face the revealed dangers. In addition, the final part also identified three underestimated threats which were additionally supplemented by recommendations on how to be more effective in the way of prevention or mitigation of their effects on the system and users. Galileo GNSS is definitely one of the best PNT services available nowadays and its development is still ongoing, so the performance will continue to improve. According to the data, the Galileo constellation provides the most accurate service and information, helps to run the economies, and collaborates on common wealth. Since the GNSS is currently a crucial part of everyone's life, this technology must be well secured against outer influence. The new generation of G2 satellites should perform even better than the current ones which are already in orbit. Finally, interoperability with other GNSS systems allows it to exceed its limits to produce even better service than would be available in sole operation.

This diploma thesis had set three research questions which were answered throughout the previous sections. The first question: *How do the European Union Agency for the Space Programme (EUSPA) and European Space Agency (ESA) deal with possible threats to Galileo GNSS?* was elaborated from the first to the third chapter of this thesis where Galileo GNSS was described in detail, threats to satellite systems were indicated and Galileo's prevention and security measures examined. The second research question: *Is the security of Galileo GNSS prevention sufficient?* was broadly answered in the third chapter where the efficiency of the prevention measures was evaluated according to conducted tests, results of scholarly and scientific examinations, and publicly shared information about the performance, technology or initiatives by the key stakeholders such as ESA or EUSPA. It is important to highlight that many of the threats' prevention solutions are under ongoing development or validation phases so the active incorporation of such measures will even enhance the security capabilities of Galileo GNSS. The focus of the technology-based attack/prevention evaluation of sufficiency was in the field of technology research and studies where the implemented tools were under deep testing to prove them as useful or not. At the same time, the efficiency of presented solutions was also considered in the light of already experienced events of threat occurrence to reveal their usefulness. The outcome of this question led to an overall positive answer with the subsequent identification of three fields in which there should be placed focus – cyber

security, space debris, and nuclear weapons. The last research question: *What should be done more to prevent any harm to the operationalisation of Galileo GNSS?* was then analysed in the *Recommendations* section where the three indicated security threats with insufficient system prevention methods were provided specific recommendations. For the cyber security measures, advanced multi-factor authentication, advanced encryption, regular security audit and fostering a debate regarding cyber security awareness and training was recommended. For space debris, active debris removal, laser ablation usage and international regulations were put on the table. Finally, nuclear weapons mitigation and prevention measures were recommended to be multilaterally discussed over arms control and international cooperation. It is important to highlight that all the information contained in this diploma thesis and for the evaluation is from open-access sources. If any of the presented recommendations or prevention measures are already set or to be set, the information might be classified and not broadly verifiable.

According to the presented outcomes of research questions, the hypothesis: *Galileo GNSS is sufficiently secured against external threats* is approved based on the previously set boundaries of its possible approval based on achievable and implemented technology and security measures against material and technical-based threats. All the presented recommendations are rather additional possible enhancements than completely missing fields. The only partially underestimated field is the current space debris removal. ESA is focusing on the future sustainability of space missions but should not forget about the actual number of particulars orbiting the Earth that already threatens satellites and other objects. In conclusion, Galileo GNSS is one of the most advanced technologies serving humanity's growth and wealth. Its PNT service provision is crucial for many fields and as such, the European Union and ESA/EUSPA must continuously improve not only its service, but also security.

Bibliography

Aerospace Technology (2012). *ESA's second pair of Galileo satellites launched into orbit.* Aerospace Technology. Available at: https://www.aerospace-technology.com/uncategorised/newsesas-second-pair-galileo-satellites-launched-into-orbit/. (Accessed: 12 Nov 2022).

Airbus (2022). *Galileo 2nd generation satellites ready to navigate into the future*. Airbus. Available at: https://www.airbus.com/en/newsroom/press-releases/2022-03-galileo-2nd-generation-satellites-ready-to-navigate-into-the-future. (Accessed: 26 Nov 2022).

Arianespace (2022). *Arianespace to launch eight new Galileo satellites*. Arianespace. Available at: https://www.arianespace.com/press-release/arianespace-to-launch-eight-new-galileo-satellites/. (Accessed: 13 Nov 2022).

Bartolomé, J. P., Maufroid, X., Hernández, I. F., López Salcedo, J. A., & Granados, G. S. (2015). Overview of Galileo system. In *GALILEO Positioning Technology,* pp. 9-33. Springer, Dordrecht.

Bonnor, N. (2011). A Brief History of Global Navigation Satellite Systems. *Journal of Navigation, 65*(01), pp. 1-14. doi:10.1017/s0373463311000506

Borell, J. (2022). *Space and defence: protecting Europe and strengthening our capacity to act*. European External Action Service. Available at: https://www.eeas.europa.eu/eeas/space-and-defence-protecting-europe-and-strengthening-our-capacity-act_en. (Accessed: 19 Feb 2023).

Boyce, B. (2019). Twenty-First Century Deterrence in the Space War-Fighting Domain: Not Your Father's Century, Deterrence, or Domain. *Air & Space Power Journal*, *35*(1), pp. 34-49.

Bugos, S. (2022). *Seven Countries Join ASAT Test Ban*. Arms Control Association. Available at: https://www.armscontrol.org/act/2022-11/news-briefs/seven-countries-join-asat-test-ban. (Accessed: 22 Apr 2023).

Cast Navigation (2016). *The C2 Divide – How Obscura can Interfere with Coincident Situation Awareness*. Cast Navigation. Available at: https://castnav.com/the-c2-divide-how-obscura-can-interfere-with-coincident-situational-awareness/. (Accessed: 27 Nov 2022).

Cesari, L. Z., Carlo, A., Mantı, N. P., & Roux, L. (2021). *Space as NATO's Operational Domain: The Case of the Cyber Threats against GNSS.* 72nd International Astronautical Congress (IAC), Dubai, United Arab Emirates, 25-29 October 2021.

Chen, S. (2022). *Chinese military scientists simulated a nuclear blast in space to knock out satellite networks like Starlink*. Business Insider. Available at: https://www.businessinsider.com/chinese-scientists-simulate-space-nuclear-blast-to-take-out-satellites-2022-10. (Accessed: 10 Dec 2022).

Cheng, N., Song, S., & Xie, H. (2019). Investigation of Solar Flares Impact on GPS/BDS/GALILEO Broadcast Ionospheric Models. *Radio Science, 54*(1), pp. 91-103. doi: 10.1029/2018RS006591

Conrad, E. E., Gurtman, G. A., Kweder, G., Mandell, M. J., & White, W. W. (2010). *Collateral damage to satellites from an EMP attack*. Defense Threat Reduction Agency, Fort Belvoir, VA.

Cozzens, T. (2021). *Galileo satellite performs collision avoidance maneuver*. GPS World. Available at: https://www.gpsworld.com/galileo-satellite-performs-collision-avoidance-maneuver/. (Accessed: 15 Apr 2023).

Curran, J. T., & Paonni, M. (2014). Securing GNSS: An end-to-end feasibility analysis for the Galileo open-service. In *Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014)*, pp. 2828-2842. doi: 10.13140/2.1.4166.0163

Dawson, M., Wright, J., & Omar, M. (2015). Mobile devices: The case for cyber security hardened systems, in Dawson, M., and Omar, M. (ed.) *New Threats and Countermeasures in Digital Crime and Cyber Terrorism*. IGI Global, pp. 8-29.

De Bakker, P. F., Samson, J., Joosten, P., Spelat, M., Hoolreiser, M., & Ambrosius, B. (2006). Effect of radio frequency interference on GNSS receiver output. *Proceedings of the 3rd ESA Workshop on Satellite Navigation User Equipment Technologies (NAVITEC'06).*

De Ingenieur (2018). *After 13 years, Galileo Satellite Navigation complete at last*. De Ingenieur. Available at: https://www.deingenieur.nl/artikel/after-13-years-galileo-satellite-navigation-complete-at-last. (Accessed: 18 Dec 2022).

De Selding, P. B. (2010). *European Officials Poised To Remove Chinese Payloads From Galileo Sats*. SpaceNews. Available at: https://spacenews.com/european-officials-poised-remove-chinese-payloads-galileo-sats/. (Accessed: 08 Apr 2023).

Dutta, P., Halder, T., Banerjee, S., Basak, A., Nanda, S., & Chakravarty, D. (2022). Analysis of jamming and anti jamming techniques for Galileo GNSS. *Materials Today: Proceedings*, *58*, pp. 489-495. doi: 10.1016/j.matpr.2022.03.009

Ellison, N. (2018). *Five Ways You Can Reduce Human Error in the Workplace*. Pandle. Available at: https://www.pandle.com/blog/2018/12/11/five-ways-you-can-reduce-human-error-in-the-workplace/. (Accessed: 04 Feb 2023).

ESA (2021). *Galileo Second Generation*. The European Space Agency. Available at: https://www.esa.int/ESA_Multimedia/Images/2021/05/Galileo_Second_Generation. (Accessed: 13 Nov 2022).

ESA (2023). *Galileo: no way without time*. The European Space Agency. Available at: https://www.esa.int/Applications/Navigation/Galileo_no_way_without_time. (Accessed: 22 Apr 2023).

ESA (n.d.a). *How the Galileo atomic clocks work*. The European Space Agency. Available at: https://www.esa.int/Applications/Navigation/How_the_Galileo_atomic_clocks_work (Accessed: 05 Nov 2022).

ESA (n.d.b). *Galileo: a constellation of navigation satellites*. The European Space Agency. Available at: https://www.esa.int/Applications/Navigation/Galileo/Galileo_a_constellation_of_navigation_satellites. (Accessed: 12 Nov 2022).

ESA (n.d.c). *Galileo services.* The European Space Agency. Available at: https://www.esa.int/Applications/Navigation/Galileo/Galileo_services. (Accessed: 12 Nov 2022).

ESA (n.d.d). *Mitigating space debris generation.* The European Space Agency. Available at: https://www.esa.int/Space_Safety/Space_Debris/Mitigating_space_debris_generation. (Accessed: 19 Feb 2023).

ESA (n.d.e). *Clean Space*. The European Space Agency. Available at: https://www.esa.int/Space_Safety/Clean_Space/Clean_Space2. (Accessed: 26 Feb 2023).

ESA (n.d.f). *Galileo satellites*. The European Space Agency. Available at: https://www.esa.int/Applications/Navigation/Galileo/Galileo_satellites. (Accessed: 04 Mar 2023).

ESA (n.d.g) *Active debris removal*. The European Space Agency. Available at: https://www.esa.int/Space_Safety/Space_Debris/Active_debris_removal. (Accessed: 15 Apr 2023).

ESA (n.d.h). *Clearspace-1*. The European Space Agency. Available at: https://www.esa.int/Space_Safety/ClearSpace-1. (Accessed: 15 Apr 2023).

eoPortal (2022). *Galileo-G2*. eoPortal. Available at: https://www.eoportal.org/satellite-missions/galileo-g2#procuring-galileos-new-generation-on-the-ground. (Accessed: 01 Apr 2023).

European Commission (1999). *Communication from the commission – Galileo – Involving Europe in a New Generation of Satellite Navigation Services (COM(1999) 54)*. European Commission. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=LEGISSUM:l24205.

European Commission (2003). *Council endorses China's participation in Galileo.* European Commission. Available at: https://cordis.europa.eu/article/id/21118-council-endorses-chinas-participation-in-galileo. (Accessed: 08 Apr 2023).

European Commission (2020). *Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats.* European Commission. Available at: https://cordis.europa.eu/project/id/883284. (Accessed: 15 Apr 2023).

European Parliament (1999). Resolution on the communication from the Commission to the Council and the European Parliament 'Towards a Trans- European Positioning and Navigation Network: including a European Strategy for Global Navigation Satellite Systems (GNSS)' (COM(98)0029 C4-0188/98). *Official Journal* C104, p. 73.

European Parliament (2011). *Reasons for and advantages of Galileo*. European Parliament. Available at: https://www.europarl.europa.eu/news/en/press-room/20111017BKG29534/galileo-lift-off-eu-satellite-navigation-is-becoming-a-reality/2/reasons-for-and-advantages-of-galileo. (Accessed: 05 Feb 2023).

EUSPA (2016). *Galileo goes live*. European Union Agency for the Space Programme. Available at: https://www.euspa.europa.eu/newsroom/news/galileo-goes-live. (Accessed: 12 Nov 2022).

EUSPA (2017). *Galileo Commercial Service Implementing Decision enters into force*. European Union Agency for the Space Programme. Available at: https://www.euspa.europa.eu/newsroom/news/galileo-commercial-service-implementing-decision-enters-force. (Accessed: 12 Nov 2022).

EUSPA (2019). *European space community steps up to Security and Defence.* European Union Agency for the Space Programme. Available at: https://www.euspa.europa.eu/newsroom/news/european-space-community-steps-security-and-defence. (Accessed: 15 Apr 2023).

EUSPA (2021a). *Security*. European Union Agency for the Space Programme. Available at: https://www.euspa.europa.eu/about/what-we-do/security. (Accessed: 15 Apr 2023).

EUSPA (2021b). *Benefits.* European Union Agency for the Space Programme. Available at: https://www.euspa.europa.eu/european-space/galileo/benefits. (Accessed: 12 Mar 2023).

EUSPA (2022a). *What is SBAS?* European Union Agency for the Space Programme. Available at: https://www.euspa.europa.eu/european-space/eu-space-programme/what-sbas. (Accessed: 22 Apr 2023).

EUSPA (2022b). *System Engineer*. European Union Agency for the Space Programme. Available at: https://vacancies.euspa.europa.eu/Jobs/VacancyDetails/1649#conditions. (Accessed: 04 Feb 2023).

EUSPA (2023a). *Search and Rescue (SAR) / Galileo Service*. European Union Agency for the Space Programme. Available at: https://www.euspa.europa.eu/european-space/galileo/services/search-and-rescue-sar-galileo-service. (Accessed: 22 Apr 2023).

EUSPA (2023b). *What is EGNOS?* European Union Agency for the Space Programme. Available at: https://www.euspa.europa.eu/european-space/egnos/what-egnos. (Accessed: 08 Apr 2023).

Fehner, T. R., & Gosling, F. G. (2006). *Atmospheric Nuclear Weapons Testing*. United States Department of Energy. Available at: https://www.energy.gov/management/articles/fehner-and-gosling-atmospheric-nuclear-weapons-testing-1951-1963-battlefield. (Accessed: 08 Apr 2023).

Fernandez-Hernandez, I., Damy, S., Cancela-Diaz, S., Chamorro-Moreno, A., Calle-Calle, J. D., Susi, M., Martini, I., Winkel, J. Ó., de Blas, J., Simón, J., Blonski, D., & Ibanez Izquierdo, D. (2023). *Galileo Authentication and High Accuracy: getting to the Truth.* Inside GNSS. Available at: https://insidegnss.com/galileo-authentication-and-high-accuracy-getting-to-the-truth/. (Accessed: 18 Mar 2023).

Foye, H., & Hernández, G. R. (2022). *UN First Committee Calls for ASAT Test Ban*. Arms Control Association. Available at: https://www.armscontrol.org/act/2022-12/news/un-first-committee-calls-asat-test-ban. (Accessed: 26 Feb 2023).

Gkotsis, I., Perlepes, L., Aggelis, A., Valouma, K., Kostaridis, A., Georgiou, E., ... & Mantzana, V. (2023). Solutions for Protecting the Space Ground Segments: From Risk Assessment to Emergency Response. In *Computer Security. ESORICS 2022 International Workshops: CyberICPS 2022, SECPRE 2022, SPOSE 2022, CPS4CIP 2022, CDT&SECOMANE 2022, EIS 2022, and SecAssure 2022, Copenhagen, Denmark, September 26–30, 2022, Revised Selected Papers* (pp. 291-307). Cham: Springer International Publishing.

Global Resilience Institute at Northeastern University (n.d.). *Space debris poses growing threat to satellite infrastructure*. Global Resilience Institute at Northeastern University. https://globalresilience.northeastern.edu/space-debris-poses-growing-threat-to-satellite-infrastructure/. (Accessed: 04 Dec 2022).

GPS.gov (n.d.). *Other Global Navigation Satellite Systems (GNSS).* GPS.gov. Available at: https://www.gps.gov/systems/gnss/. (Accessed: 18 Dec 2022).

GPS World (2011). *Galileo IOV Satellites Successfully Launched into Orbit*. GPS World. Available at: https://www.gpsworld.com/gnss-systemgalileonewsgalileo-iov-satellites-succesfully-launched-orbit-12211/. (Accessed: 12 Nov 2022).

GPS World (2014). *Galileo Achieves In-Orbit Validation*. GPS World. Available at: https://www.gpsworld.com/galileo-achieves-in-orbit-validation/. (Accessed: 12 Nov 2022).

GSC (n.d.a). *GNSS Emergency Warning Service successfully tested*. European GNSS Service Centre. Available at: https://www.gsc-europa.eu/news/gnss-emergency-warning-service-successfully-tested. (Accessed: 22 Apr 2023).

GSC (n.d.b). *Galileo High Accuracy Service (HAS)*. European GNSS Service Centre. Available at: https://www.gsc-europa.eu/galileo/services/galileo-high-accuracy-service-has. (Accessed: 12 Nov 2022).

GSC (n.d.c). *Constellation Information*. European GNSS Service Centre. Available at: https://www.gsc-europa.eu/system-service-status/constellation-information. (Accessed: 01 Apr 2023).

GSC (n.d.d). *System.* European GNSS Service Centre. Available at: https://www.gsc-europa.eu/galileo/system. (Accessed: 13 Nov 2022).

GSC (n.d.e). *Galileo Open Service Navigation Message Authentication (OSNMA).* European GNSS Service Centre. Available at: https://www.gsc-europa.eu/galileo/services/galileo-open-service-navigation-message-authentication-osnma. (Accessed: 05 Feb 2023).

Gurzu, A., & Posaner, J. (2019). *Galileo blackout followed effort to guard against cyber threats*. Politico. Available at: https://www.politico.eu/article/galileo-blackout-followed-effort-to-guard-against-cyber-threats/. (Accessed: 18 Mar 2023).

Gustafsson, J. (2017). *Single case studies vs. multiple case studies: A comparative study*. Halmstad University, School of Business, Engineering and Science.

Gutierrez, P. (2022). *Brussels View: EU Space Community Talks Security, Defense and Galileo*. Inside GNSS. Available at: https://insidegnss.com/brussels-view-eu-space-community-talks-security-defense-and-galileo/. (Accessed: 12 Feb 2023).

Harrison, T., Cooper, Z., Johnson, K., & Roberts, T. G. (2017). *Escalation and deterrence in the second space age.* Rowman & Littlefield.

Hayes, E. (2022). *The Bohu Laser Facility, Part 2: Operations*. Arms Control Wonk. Available at: https://www.armscontrolwonk.com/archive/1216867/the-bohu-laser-facility-part-2-operations/. (Accessed: 22 Apr 2023).

Hennink, M., Hutter, I., & Bailey, A. (2020). *Qualitative research methods*. Sage.

Hlubek, N., Berdermann, J., Wilken, V., Gewies, S., Jakowski, N., Wassaie, M., & Damtie, B. (2014). Scintillations of the GPS, GLONASS, and Galileo signals at equatorial latitude. *Journal of Space Weather and Space Climate, 4*, pp. 1-7. doi: 10.1051/swsc/2014020

Hollinger, P., & Learner, S. (2022). *How space debris threatens modern life*. Financial Times. Available at: https://ig.ft.com/space-debris/. (Accessed: 04 Dec 2022).

Inside GNSS (2016). *Interference Mitigation in the E5a Galileo Band Using an Open Source Simulator.* Inside GNSS. Available at: https://insidegnss.com/interference-mitigation-in-the-e5a-galileo-band-using-an-open-source-simulator/. (Accessed: 05 Feb 2023).

Inside GNSS (2021). *Enhanced BeiDou Short Message Service Displayed at International Summit.* Inside GNSS. Available at: https://insidegnss.com/enhanced-beidou-short-message-service-displayed-at-intl-summit/. (Accessed: 22 Apr 2023).

Karaim, M., Elsheikh, M., & Noureldin, A. (2018). GNSS Error Sources, in Rustamov, R. B., and Hashimov, A. M. (ed.) *Multifunctional Operation and Application of GPS*, IntechOpen, pp. 69-85.

Kay, T. (2022). *Counterspace Weapons 101*. Aerospace Security. Available at: https://aerospace.csis.org/aerospace101/counterspace-weapons-101/. (Accessed: 04 Mar 2023).

Klein, J. J., & Boensch, N. J. (2020). Role of Space in Deterrence, in Schrogl, K.-U. (ed.) *Handbook of Space Security: Policies, Applications and Programs*, Springer Reference, pp. 111-126.

Kluth, A. (2023). *The International Space Station Is a Model for a Better World*. The Washington Post. Available at: https://www.washingtonpost.com/business/2023/04/15/the-international-space-station-is-a-model-for-a-better-world/f7fb09a2-db54-11ed-aebd-3fd2ac4c460a_story.html. (Accessed: 15 Apr 2023).

Kos, T., Markezic, I., & Pokrajcic, J. (2010). Effects of multipath reception on GPS positioning performance. *Proceedings EPLMAR-2010*, pp. 399-402. IEEE.

Kramer, J. H. (n.d.a). *GIOVE-A (Galileo In-Orbit Validation Element-A).* eoPortal. Available at: https://www.eoportal.org/satellite-missions/giove-a#spacecraft. (Accessed: 05 Nov 2022).

Kramer, J. H. (n.d.b). *GIOVE-B (Galileo In-Orbit Validation Element-B).* eoPortal. Available at: https://www.eoportal.org/satellite-missions/giove-b#congo-cooperative-network-for-giove-observation. (Accessed: 05 Nov 2022).

Langley, R. B., Teunissen, P. J., & Montenbruck, O. (2017). 'Introduction to GNSS', in Teunnisen, P., & Montenbruck, O. (ed.) *Springer handbook of global navigation satellite systems.* Springer, Cham, pp. 3-23.

Lannelongue, S., Guichon, H., Benniguel, Y., Crisci, M., & Amarillo, F. (2008). *Characterisation of Scintillation effect on Galileo Sensor Station Continuity of Service*. IEEA. Available at: http://www.ieea.fr/publications/ieea-2008-gnss.pdf. (Accessed: 12 Mar 2023).

Lindström, G., & Gasparini, G. (2003). *The Galileo satellite system and its security implications*. Inst. for Security Studies.

Liu, Z., Lin, C., & Chen, G. (2020). Space Attack Technology Overview. *Journal of Physics: Conference Series, 1544*(1). doi: 10.1088/1742-6596/1544/1/012178

Lopez, G., & Simsky, M. (2021). *What is GNSS Spoofing?* GIM International. Available at: https://www.gim-international.com/content/article/what-is-gnss-spoofing. (Accessed: 03 Dec 2022).

Matias, J. C. (2007). E.U.-China Partnership on the Galileo Satellite System: Competing with the U.S. in Space. *The Asia-Pacific Journal, 5*(7). Available at: https://apjjf.org/-Jose-Carlos-Matias/2473/article.html. (Accessed: 08 Apr 2023).

Mehta, P. (2022). *Solar storms can destroy satellites with ease – a space weather explains the science.* The Conversation. Available at: https://theconversation.com/solar-storms-can-destroy-satellites-with-ease-a-space-weather-expert-explains-the-science-177510. (Accessed: 05 Mar 2023).

Moltz, J. C. (2011). *Coalition Building in Space: Where Networks are Power*. Naval Postgraduate School Monterey CA.

Mowthorpe, M. (2023). *Space resilience and the importance of multiple orbits*. The Space Review. Available at: https://www.thespacereview.com/article/4504/1. (Accessed: 04 Mar 2023).

Mukherji, V., & Chandele, A.K.S. (2021). *GNSS Jamming: An Omnipresent Threat. Geospatial World*. Available at: https://www.geospatialworld.net/prime/special-features/gnss-jamming-an-omnipresent-threat/. (Accessed: 27 Nov 2022).

NCISA (n.d.). *What is NÚKIB / NCISA*. National Cyber and Information Security Agency. Available at: https://www.govcert.cz/en/. (Accessed: 12 Feb 2023).

Nouwens, M., & Legarda, H. (2018). *China's pursuit of advanced dual-use technologies*. International Institute for Strategic Studies. Available at: https://www.iiss.org/research-paper//2018/12/emerging-technology-dominance. (Accessed: 29 Apr 2023).

Novatel (n.d.). *What are Global Navigation Satellite Systems?* Novatel. Available at: https://novatel.com/tech-talk/an-introduction-to-gnss/what-are-global-navigation-satellite-systems-gnss. (Accessed: 21 Jan 2023).

Novelly, T. (2023). *Attack on Satellites May Trigger Military Response, US and Japanese Officials Say*. Military.com. Available at: https://www.military.com/daily-news/2023/01/12/attacks-satellites-may-trigger-military-response-us-and-japanese-officials-say.html. (Accessed: 19 Feb 2023).

Nuclear Threat Initiative (n.d.). *Partial Test Ban Treaty (PTBT)*. Nuclear Threat Initiative. Available at: https://www.nti.org/education-center/treaties-and-regimes/treaty-banning-nuclear-test-atmosphere-outer-space-and-under-water-partial-test-ban-treaty-ptbt/. (Accessed: 04 Mar 2023).

Oruc, A. (2022). Potential cyber threats, vulnerabilities, and protections of unmanned vehicles. *Drone Systems and Applications*, *10*(1), pp. 51-58. doi: 10.1139/juvs-2021-0022

Parkinson, B. (2022). *Toughen GPS to resist jamming and spoofing.* GPS World. Available at: https://www.gpsworld.com/toughen-gps-to-resist-jamming-and-spoofing/. (Accessed: 18 Mar 2023).

Peeters, W. (2022). *Cyberattacks on Satellites: An Underestimated Political Threat.* The London School of Economics and Political Science. Available at: https://www.lse.ac.uk/ideas/projects/space-policy/publications/Cyberattacks-on-Satellites. (Accessed: 18 Dec 2022).

Peng, Z. (2020). *Is China's BeiDou a Better Version of GPS and GLONASS?* EqualOcean. Available at: https://equalocean.com/analysis/2020082614631. (Accessed: 18 Dec 2022).

Pražák, J. (2022). On the Threshold of Space Warfare. *Astropolitics, 20*(2), pp. 175-191. doi: 10.1080/14777622.2022.2142351

Prochniewicz, D., & Grzymala, M. (2021). Analysis of the Impact of Multipath on Galileo System Measurements. *Remote Sensing, 13*(12), 2295. doi: 10.3390/rs13122295

Psiaki, M. L., & Humphreys, T. E. (2016). GNSS spoofing and detection. *Proceedings of the IEEE, 104*(6), pp. 1258-1270. IEEE.

Qadir, S., & Quadri, S. M. K. (2016). Information availability: An insight into the most important attribute of information security. *Journal of Information Security*, *7*(3), pp. 185-194. doi: 10.4236/jis.2016.73014

Sarto, C. (2020). Galileo OSNMA for smartphones [presentation]. *Fourth annual GNSS Raw Measurements Taskforce Workshop*, Prague.

Sheik, A. T., Atmaca, U. I., Maple, C., & Epiphaniou, G. (2022). Challenges in threat modelling of new space systems: A teleoperation use-case. *Advances in Space Research*, *70*(8), pp. 2208-2226. doi: 10.1016/j.asr.2022.07.013

Shevchenko, N., Chick, T. A., O'Riordan, P., Scanlon, T. P., & Woody, C. (2018). *Threat modelling: a summary of available methods*. Carnegie Mellon University Software Engineering Institute Pittsburgh United States.

Shuangyan, S., Xing, J., & Hao, C. (2014). Cleaning space debris with a space-based laser system. *Chinese Journal of Aeronautics, 27*(4), pp. 805-811. doi: 10.1016/j.cja.2014.05.002

Simsky, M. (2019). *How do we ensure GNSS security against spoofing?* GPS World. Available at: https://www.gpsworld.com/how-do-we-ensure-gnss-security-against-spoofing/. (Accessed: 05 Feb 2023).

Sindon, J. (n.d.). *GNSS Security and Cybersecurity: What are the Parallels?* Orolia. Available at: https://www.orolia.com/gnss-security-and-cybersecurity-what-are-the-parallels/. (Accessed: 12 Feb 2023).

Sitruk, A., & Plattard, S. (2017). *The Governance of Galileo*. European Space Policy Institute.

Space Weather Prediction Center (n.d.). *Ionospheric Scintillation*. National Oceanic and Atmospheric Administration. Available at: https://www.swpc.noaa.gov/phenomena/ionospheric-scintillation. (Accessed: 27 Nov 2022).

Spirent (2018). *Fundamentals of GPS Threats*. Spirent. Available at: https://www.spirent.com/assets/wp-fundamentals-of-gps-threats. (Accessed: 27 Nov 2023).

Srour, L. (2022). *Who is going to take out the trash? Addressing space debris under international law.* Public International Law and Policy Group. Available at: https://www.publicinternationallawandpolicygroup.org/lawyering-justice-blog/2022/3/14/who-is-going-to-take-out-the-trash-addressing-space-debris-under-international-law. (Accessed: 26 Feb 2023).

Stephenson, P. (2012). Talking space: The European Commission's changing frames in defining Galileo. *Space Policy*, *28*(2), pp. 86-93. doi: 10.1016/j.spacepol.2012.02.011

SWE (n.d.). *Space Weather at ESA*. ESA Space Weather. Available at: https://swe.ssa.esa.int/ssa-space-weather-activities. (Accessed: 15 Apr 2023).

Syam, W. (2022). *Meaconing: the most common type of GNSS spoofing interference attack.* Wasy Research. Available at: https://www.wasyresearch.com/meaconing-the-most-common-type-of-gnss-spoofing-interference-attacks/. (Accessed: 22 Apr 2023).

Tellis, A. J. (2019). *India's ASAT Test: An Incomplete Success.* Carnegie Endowment for International Peace. Available at: https://carnegieendowment.org/2019/04/15/india-s-asat-test-incomplete-success-pub-78884. (Accessed: 08 Apr 2023).

Thales Alenia Space (2021). *Thales Alenia Space will play a major role on-board Galileo 2nd Generation and will boost performance and cybersecurity for the constellation.* Thales Alenia Space. Available at: https://www.thalesgroup.com/en/worldwide/space/press-

release/thales-alenia-space-will-play-major-role-board-galileo-2nd-generation. (Accessed: 26 Nov 2022).

Timbrook, R. (2021). *GPS Vs. GLONASS Vs. Galileo: What's The Best GNSS?* Expert World Travel. Available at: https://expertworldtravel.com/gps-vs-glonass-vs-galileo/. (Accessed: 18 Dec 2022).

Tingley, B. (2022). *Satellites spot construction of Russian anti-satellite laser facility: report.* Space.com. Available at: https://www.space.com/russia-anti-satellite-laser-facility-satellite-photos. (Accessed: 10 Dec 2022).

Torr, P. (2005). Demystifying the threat modelling process. *IEEE Security & Privacy*, *3*(5), pp. 66-70. doi: 10.1109/MSP.2005.119

Vadakke Veettil, S., Aquino, M., Marques, H. M., & Moraes, A. (2020). Mitigation of ionospheric scintillation effects on GNSS precise point positioning (PPP) at low latitudes. *Journal of Geodesy, 94*(15). doi: 10.1007/s00190-020-01345-z

Van Rees, E. (2021). *Galileo OSNMA: the latest GNSS anti-spoofing technique*. GeoConnexion. Available at: https://www.geoconnexion.com/news/galileo-osnma-the-latest-gnss-anti-spoofing-technique. (Accessed: 05 Feb 2023).

United Nations (2022). '*We Have Not Passed the Point of No Return', Disarmament Committee Told, Weighing Chance Outer Space Could Become Next Battlefield.* UGA/DIS/3698. United Nations. Available at: https://press.un.org/en/2022/gadis3698.doc.htm.

Zervos, V., & Siegel, D. S. (2008). Technology, security, and policy implications of future transatlantic partnerships in space: Lessons from Galileo. *Research Policy*, *37*(9), pp. 1630-1642. doi: 10.1016/j.respol.2008.06.008

List of Abbreviations

ADR	Active debris removal
ASAT	Anti-Satellite Weapon Test
EGNOS	European Geostationary Navigation Overlay Service
ESA	European Space Agency
EU	European Union
EUSPA	European Union Agency for the Space Programme
FOC	Full Operational Capability
G2	Galileo Generation 2 satellites
GEO	Geostationary Equatorial Orbit
GNSS	Global Navigation Satellite System
GSC	European GNSS Service Centre
IOV	In-Orbit Validation phase
MEO	Medium Earth Orbit
NLMS	Normalized Least Mean Square
LEO	Low Earth Orbit
OSNMA	Open Service Navigation Message Authentication
PNT	Positioning, Navigation and Timing
PTBT	Partial Test Ban Treaty
SWE	ESA Space Weather
UN	United Nations