UNIVERSITA' POLITECNICA DELLE MARCHE

FACOLTA' DI INGEGNERIA

Corso di Laurea Magistrale in Ingegneria Elettronica

ATT4S, a knowledge base of Adversaries Tactics and Techniques for Space

ATT4S, una base di conoscenza di Tattiche e Tecniche Avversarie per lo Spazio

Internship at the European Space Agency, ESTEC, NL

Relatore:

Dr. **Massimo Battaglioni**

Candidato:

Francesco Traini

Correlatore:

Prof. **Luca Spalazzi**

A.A. **2021-2022**

To my aunt Carla,
without whom this internship - and so this thesis - would have never been possible.
In loving memory.

ACKNOWLEDGEMENTS

First of all, I would like to thank the supervisor of my internship experience in ESA, Dr. Antonios Atlasis, who offered me this opportunity and this project. He worked with me, supported, and supervised me during the internship and the preparation of the thesis. Without his assistance and involvement in every step of the work, this thesis would have never been accomplished. I would like to thank also the whole TEC-ESS section, of which I was part and which hosted me during the project duration.

I would also like to show my gratitude to my academic supervisors, Dr. Massimo Battaglioni and Prof. Luca Spalazzi, for the revision of this thesis. Dr. Battaglioni has been essential for his constant and necessary support during the drafting of this thesis.

This thesis is the finish line of five years of exciting study path, made with my indispensable University travelling companions: Alessio, Daniele, Laura, the two Lorenzos and Michele are only some of them, who made University an enjoyable and unforgettable life experience.

My thanks go to my best friends and life companions, who accompanied and encouraged me during my daily life. Giacomo, Mirko, Serena, Silvia, but not only them.

None of this could have been possible without my family. Constant reference point, they always believed in me, giving me precious advice during my most important choices. My gratitude and love will be always for them.

ABSTRACT

There is no doubt Security is today on top of the priority list of every organization, for every type of system. This is also valid for the space industry, which has been enormously growing in recent years. The European Space Agency owns and operates on some of the most important space assets for provided services, and it is actively working to protect all of them, guaranteeing security and the consequent safety of involved people.

Although space systems need a work on security comparable, if not higher than, to IT systems, and the existing constraints are important, a lack on standard security frameworks is manifest. The available tools and frameworks are not tailored to space systems and are inadequate to cover the relevant existing divergences.

This work aims to produce a framework to model threats, representing them as specific actions, called Techniques, performed by adversaries against a system. The considered reference product, developed for IT systems and taken in this work as an example to produce an equivalent structure for Space, is the MITRE ATT&CK® [1] set of matrices.

Existing Techniques have been selected, and new ones have been created by studying related publications, reports, CCSDS standards, and gathering knowledge from experts in ESA.

The result is ATT4S, Adversaries Tactics and Techniques for Space, a structured collection of knowledge in the shape of a matrix, that can be used as a support for Risk Management, to identify threats and to decide how to face them. In addition to Techniques, some possible Mitigations are provided, to reduce the possible impact of attacks.

A Website is available - currently only for ESA internal network – to navigate the matrix and work with it.

ATT4S has been presented to Security WG during the CCSDS Fall 2022 Meetings, and it is currently under further development by the System Security section in ESA.

ABSTRACT ESTESO ITALIANO

La sicurezza è indubbiamente tra le principali preoccupazioni di qualsiasi organizzazione, indipendentemente dalla tipologia di sistema implementato. La stessa assunzione è valida per il settore spaziale, in costante crescita negli ultimi anni. L'Agenzia Spaziale Europea (ESA) possiede e gestisce alcune tra le più importanti risorse spaziali dal punto di vista dei servizi forniti, ed è al lavoro anch'essa per garantir loro un'adeguata protezione, e di conseguenza la sicurezza delle persone coinvolte.

Nonostante i requisiti di sicurezza richiesti dai sistemi spaziali siano equivalenti, quando non maggiori, dei sistemi IT, e nonostante molte limitazioni siano presenti, si evidenzia un'importante carenza negli standard di sicurezza esistenti. Gli strumenti e i framework disponibili non considerano le specificità dei sistemi spaziali, e sono inadeguati a coprire le differenze esistenti.

L'obiettivo di questo lavoro è un framework per modellare le minacce, rappresentandole come azioni specifiche dette Tecniche, che possono essere eseguite da un attaccante contro un sistema. Il riferimento dal quale si è partiti è il set di matrici di MITRE ATT&CK [1], preso come esempio per riprodurre una simile struttura per lo Spazio.

Si è proceduto con la selezione di specifiche Tecniche, e delle nuove sono state create attingendo da pubblicazioni, report, standard CCSDS ed intervistando esperti dell'ESA.

Il risultato è ATT4S - acronimo di Adversaries Tactics and Techniques for Space - una raccolta organizzata e strutturata in forma matriciale, che può essere utilizzata per supportare le operazioni di gestione del rischio, per identificare le minacce e decidere come affrontarle. Inoltre, sono state anche inserite possibili Mitigazioni, utilizzabili per ridurre il potenziale impatto degli attacchi.

È disponibile, ma al momento solo all'interno della rete locale ESA, un sito web per navigare ed utilizzare la matrice.

ATT4S è stato presentato al Security WG dei CCSDS Fall 2022 Meetings, ed è tuttora in corso di sviluppo dalla sezione System Security dell'ESA.

INDEX

LIST OF FIGURES

ABBREVIATIONS

AES	Advanced Encryption Standard
AiTM	Adversary-in-The-Middle
API	Application Programming Interface
APT	Advanced Persistent Threat
ASAT	Anti-Satellite
ASIC	Application-Specific Integrated Circuit
C&S	Coding and Synchronization
CA	Certificate Authority
CCSDS	the Consultative Committee for Space Data Systems
CLTU	Communications Link Transmission Unit
COTS	Commercial-Off-The-Shelf
DoS	Denial of Service
DSSS	Direct Sequence Spread Spectrum
ECSS	European Cooperation for Space Standardization
ESA	European Space Agency
FPGA	Field Programmable Gate Array
GS	Ground Station
HW	Hardware
ICS	Industrial Control System
ISP	Internet Service Provider
ISS	International Space Station
IT	Information Technology
JSON	JavaScript Object Notation
KMS	Key Management System
LAN	Local Area Network
LEO	Low Earth Orbit
LoS	Line of Sight
MAC	Media Access Control
MCS	Mission Control System
MEO	Medium Earth orbit
MiTM	Man-in-The-Middle

MMU	Memory Management Unit
MPU	Memory Protection Unit
NMA	Navigation Message Authentication
OBC	On-Board Computer
OBCP	On-Board Control Procedures
OBSW	on-board Software
OTAR	Over-The-Air rekeying
PUS	Packet Utilization Standard
QKD	Quantum Key Distribution
RF	Radio Frequency
SDLS	Space Data Link Security
SDR	Software-Defined Radio
SPARTA	Space Attack Research & Tactic Analysis
STIX	Structured Threat Information eXpression
SW	Software
TC	Telecommand
TM	Telemetry
TT&C	Tracking, Telemetry, and Command
TTPs	Tactics, Techniques, and Procedures
WG	Working Group

1 - INTRODUCTION

1.1 - CONTEXT

In recent decades, every organization has relied almost completely on information technology, and most of them use information systems in all phases of daily work. Digitalization and all related services have strengthened companies' capabilities and boosted productivity and efficiency.
This remark concerns all typology of organizations, either public and private, from civil to military sector, big companies, and the small ones.

On the other side, this dependence could cause problems if an information system is jeopardized by a threat resulting in harmful events, like loss of information, systems integrity, or availability of services. Threats derive from harmful actions, either voluntary or accidentally, caused by a malicious actor or a mistake of a user or a developer. The information security risk, i.e., the risk related to information systems and their uses [2] shall be managed, to avoid or at least to limit the impact of these dangerous episodes.

1.2 – MOTIVATION

Space Infrastructure is one of the pillars of today's economy and everyday life. It is used for Communications, Navigation, Earth Observation, Air Traffic Control, and many other peaceful activities. Its protection is vital to ensure the continuation of the protection of the planet, of the human activities and its well-being.

Due to the technology evolution, and to the increased number of threats that space systems face, part of the required protection also includes cybersecurity.
Application of cybersecurity to space systems is even more challenging than for IT systems since it needs to defend complex, interconnected, and interdependent systems, located at great distances and that are targets for several threat actors.
Furthermore, during a spacecraft development, a security level robust enough to be resilient to attacks for the following 10 to 20 years must be realized, to maintain the resource secure during its entire operational time [3]. Although software components can be updated during the lifetime of the spacecraft, it is impossible to replace hardware components, and this is a limitation for the security capabilities.

In the past decades, technologies capable to interfere with a space mission were rare, and only few governments were capable to access Space. Security was based to some extent to the impossibility to reach the system to attack it and the lack of public knowledge of the project implementation, making the *security through obscurity* effective. However, nowadays, this concept is not acceptable as a security principle.

In recent years, in fact, a new era for Space begun. Lots of private companies have started to invest in the space environment to deliver new and better services to the public. This revolution, called *New Space*, is bringing in orbit thousands of small and less expensive satellites, characterized by commercially available hardware and software [4]. The employed components are easy to find in the market, and the operating systems are more complex and vulnerable than usual. Space resources are designed to reduce expenses, and the resulting cyber defenses are not always strong enough.

On the other hand, the enormous interest in this domain simplifies the access to Space: many hardware and protocol implementations are available, and ground stations are accessible as a commercial service. Today it is increasingly easy to find the knowledge and skills to perform an attack, and many hardware resources are also available. The old approach of the security through obscurity is not effective anymore.

To address the aforementioned challenges, a Cyber Threat Intelligence approach is needed to produce a characterization of attack methods and the adversary behavior; nevertheless, there is a lack of a large collection of standards and frameworks for space systems.

For example, IT or industrial systems threats can be modelled by relying on frameworks like ATT&CK, to track and analyze the TTPs (Tactics, Techniques, and Procedures) used by APT (Advanced Persistent Threats). Although this framework covers disparate technological environments [5], the space environment is not addressed, and the need for an adversary attack matrix emerged.

1.3 – OBJECTIVE AND SETTING

The project described in this thesis has been developed during a six-month internship at the European Space Research and Technology Centre of the European Space Agency, in Noordwijk, NL. The TEC-ESS section (System Security Engineering section), headed by Dr. Antonios Atlasis who supervised and worked together for the project, offered me this topic for study in the security field.

The objective of this study is to fill the existing gap in space security frameworks by producing a matrix that models Tactics and Techniques for space, resulting in a framework that can be used in the space domain to strengthen its security level, following the concept of the ATT&CK framework. The result of this work, carried out with Dr. Atlasis and with the help of ESA experts, has been called ATT4S, which stands for Adversaries Tactics and Techniques for Space.

To the best of our knowledge, the only similar and contemporaneous work is Aerospace Corporation's Space Attack Research & Tactic Analysis (SPARTA) [6]. SPARTA is a framework built for the same purpose as the ATT4S framework, aiming to cover the absence of a tailor-made tool for Space. It has been built, according to the authors, following a top-down approach, starting from the literature related to space threats and protocols, descending to the practical techniques.
The result is comparable and partially overlapping with ATT4S, but the approach followed is different. ATT4S stems from the same philosophy, but it also comes from the opposite direction: the Enterprise matrix has been studied, and all the Techniques applicable to Space Systems have been selected and added to our matrix.

The development of ATT4S and SPARTA started and ran in parallel; Antonios Atlasis, Ignacio Aguilar Sanchez, and I contributed opinions and advice to SPARTA.
Bot were presented at the Security WG during the CCSDS Fall 2022 Meetings, where Dr. Atlasis presented ATT4S; on the date of conclusion of this thesis, February 2022, the SPARTA matrix is published online, while ATT4S is currently under development.

1.4 – OVERVIEW

The thesis is organized in 9 chapters. After this introduction, an explanation of the Risk Management process is given, followed by an outline of the space system layout.

The main research findings on threats to Space are presented in the following chapter, highlighting the main differences with ground IT systems.

After a description of the ATT&CK matrix structure, and an elucidation of the reason why a similar tool is essential for Space, the related Techniques and Mitigations are shown and described.

Then, the resulting ATT4S matrix is presented, either in its structure and in the graphical view on the website. Some helpful tools to work with the matrix and an example of a real attack representation with ATT4S can be found in the final chapters.

2 - RISK MANAGEMENT

The meaning of risk is well known to everyone and corresponds to “the possibility that something bad or unpleasant (such as an injury or a loss) will happen” [7]. Particularly for organizations, a risk is more related to damages that can affect owned assets and business. Two similar definitions come from NIST: “Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence” [8] and from ISO: “The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.” [9]

In all three cases, risk is explained with the terms “possibility” and “potential”. It denotes an event that cannot be predicted, and that may never happen. Nevertheless, it shall be handled and limited with a process called Risk Management.

According to NIST, **Risk Management** is constituted by four components: Risk Framing, Risk Assessment, Risk Response and Risk Monitoring. The four steps have a logic order of execution, but they are not completely sequential, because of their complex interaction (Figure 1). Every step can raise feedbacks and lead to the need to reexamine the previous one [2].

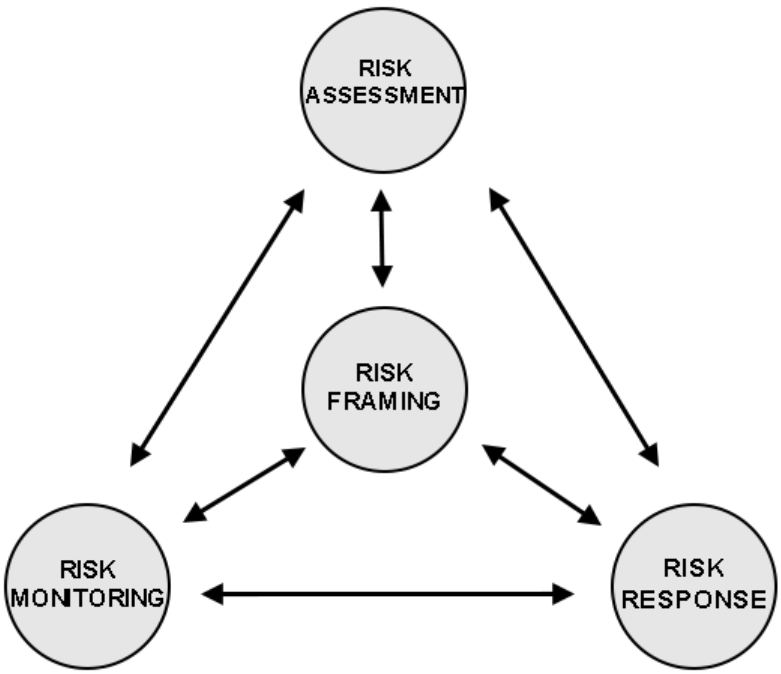

FIGURE 1 – THE FOUR STEPS OF RISK MANAGEMENT.

2.1 - RISK FRAMING

The first step of Risk Management, i.e., **Risk Framing**, is necessary to contextualize the environment to protect, producing a strategy to determine and prioritize decisions, to evaluate, monitor and manage risk.

The Risk Framing step takes laws and regulations, contractual relationships, and financial availabilities as input, which may direct or limit risk decisions.

The results of such analysis derive from an initial study of the system to be protected and may be influenced or modified by subsequent steps. The original assumptions, constraints and priorities can be changed after the Risk Assessment, that may bring out new unconsidered adversaries or vulnerabilities. New alternative choices may emerge during the Risk Response step, some of which may be ineffective or no longer needed during Risk Monitoring.

2.2 - RISK ASSESSMENT

The second component, the **Risk Assessment**, is performed to identify and analyze security risks for an organization and is divided in two phases: the Threat and Vulnerability identification, and the Risk Determination.

The first phase consists of the identification of threats that may menace assets and looking for system vulnerabilities. Threat sources are evaluated with the capabilities and intentions of the threat actors, identified by their tactics, techniques, and procedures. Vulnerabilities can be found in hardware, software, firmware, or in the environment surrounding the system, and they can result from organizational flaws, mistakes in design or process definition, or weaknesses in information systems. The exploitation of these vulnerabilities leads to a damage to the system, called impact.

The evaluation of the impact degree is estimated in the second phase, the Risk Determination. Starting from the statistical or the assumed likelihood that a malicious actor exploits a known vulnerability, and considering the resulting impact, it is possible to calculate, either quantitatively or qualitatively, the risk for the organization and its assets. The methodology of assessment, the depth and the detail of the threat analysis are input of this step, coming from the Risk Framing. The results of this step coordinate the Risk Response actions, and if the residual risk is deemed too high, a new risk assessment may be required.

2.3 - RISK RESPONSE

The third component of Risk Management, the **Risk Response**, explains how organizations respond to risk, employing the results of the previous steps to limit the possible damage. An evaluation of possible courses of actions is performed, and the selected possibilities are implemented. Several options are available to respond to risk: it can be *accepted*, *avoided*, *mitigated*, *shared*, or *transferred*.

A risk can be *accepted* if it is below a threshold, due to an extremely low likelihood or damage. However, a risk can also be accepted in an emergency if a result is needed quickly. This kind of decisions are based on a trade-off between prevention expenses and risk of damages.

If a risk is *avoided*, the activities or the technologies that cause it are avoided or redesigned to eliminate a risk that is unacceptable or unmanageable for the organization.

A part of the risk can be managed, aiming to eliminate or reduce it. This task is fulfilled with the *mitigation*, in which specific measures are put in place to produce an effective response to the risk. Security controls on the system or user' behavior, changes in the process structure, or technical countermeasures reduce the magnitude of the risk.

Sharing and *transferring* are selected when is preferred to assigning the liability and the responsibility related to risk to another organization. Risk Transfer does not reduce the likelihood of risk or its consequences; however, the organization is relieved from economical and legal troubles if an insurance is used. Risk Sharing allows the increased expertise of other companies to be leveraged against threats.

2.4 - RISK MONITORING

The last component, **Risk Monitoring**, shall be executed during the whole lifecycle of the system. Its role is the continuous monitoring of the effectiveness of risk response measures, the fulfillment of security requirements, and the identification of changes in the way risk impacts the system.

The effort of monitoring activities is outlined taking into account the results of the risk framing phase. As a secondary result, the information related to risk and threats increases risk awareness and can be used for further study and measures.

3 - SPACE SYSTEM LAYOUT

A Space infrastructure is a complex system, constituted by multiple components; some of them are mission-specific and may participate only sometimes. For example, the human component is a peculiarity of few missions, mainly related to Space stations, like the ISS.

The main components of a Space System are the Space Segment, the Transfer Segment, and the Ground Segment [10], as shown in Figure 2.

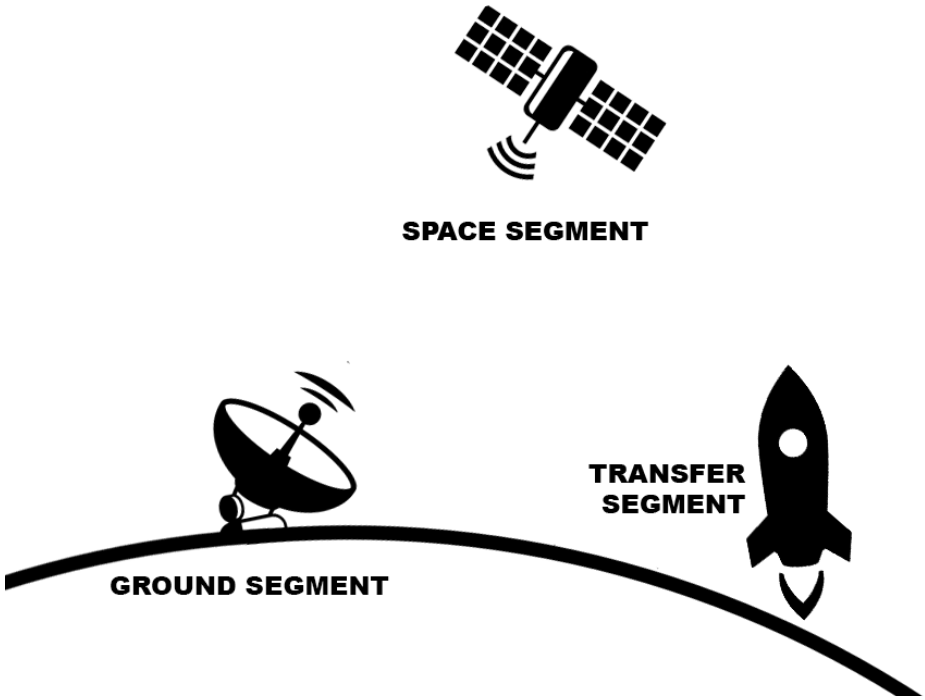

FIGURE 2 – THE THREE MAIN COMPONENTS OF A SPACE SYSTEM.

3.1 – SPACE SEGMENT

The **Space Segment** is the most important part of the system, and it is the principal peculiarity of a Space System. It can carry technology and instruments to accomplish the objective of the mission and it is composed of different sub-systems. [10]

Payload is the main element of the Spacecraft, and it is the reason of the mission itself. All the other sub-systems are built to bring the payload in orbit and keep it working.

Structure is the component that provides the mechanical support to all the other sub-systems. Movements, deployments, and other dynamic functions are also possible thanks to the structure.

Power Supply component manages the energy harvesting with solar panels or other generators, its storage with batteries and it distributes power to all the electrical devices onboard.

Communications sub-system administers the data exchange with Earth or other spacecrafts, and it is composed by a transceiver and an antenna. The exchanged data are usually divided into the TT&C (Telemetry, Tracking and Command) and the PDT (Payload Data Transmission) components. The former handles all the data exchanged in downlink to know the status of the spacecraft, its position and trajectory, and the uplink commands to govern its behavior.

Data Processing sub-system pre-processes acquired data before sending them toward the Communication channel. The purpose of this component is to properly select, and compress acquired data to fit the transmission bandwidth. The trade-off of this process is with the limited processing power and energy available onboard.

Thermal Subsystem permits to keep controlled temperatures in the different parts of the spacecraft. The side of the spacecraft facing the sun can reach high temperatures, while the shady side is extremely cold. All the components must be maintained in a defined temperature range for their safety, while some of them require a stricter working temperature to reach the highest efficiency.

Attitude Control is responsible of maintaining the spacecraft well oriented in space, using thrusters and inertial mechanisms.

Propulsion Sub-system makes use of chemical or electric thrusters to correct or change the orbit of the spacecraft, or to maintain it stable during the operational life.

Life Support System is only required for manned missions, guaranteeing a habitable environment for humans, providing clean air, water, and protections to the crew.

3.2 – TRANSFER SEGMENT

The **Transfer Segment** acts in the first stage of the mission, as a responsible of bringing the spacecraft in Space, either in orbit or not. It is composed by a launcher and a launch facility from where the launcher lifts off. There are different launchers available, made by various constructors and with dimension and thrust fitted for the various missions. The larger the mass to be launched and the higher the orbit to be reached, the more powerful the rocket must be. The launch cost is a huge limitation for accessing

Space; however, it is getting lower in recent years thanks to less expensive and even reusable launchers (SpaceX [11]).

To reduce the launch cost, Earth rotation can be leveraged, locating the launch facility close to the Equator line. Spacecraft gains a natural orbital speed, reducing the fuel required, especially if the orbit to reach is geostationary.

ESA has its own launchers, the Ariane series for heavy loads and the Vega series for lighter loads, and its own spaceport in Kourou, in French Guiana.

3.3 – GROUND SEGMENT

Ground Segment represents all the facilities and structures located on the ground that serve the spacecrafts operations. It is divided in Mission Operations and Ground Station Network.

Mission Operations are the set of procedures conducted in the control center to monitor the spacecraft conditions by analyzing telemetry, and to control its behavior during all phases of the mission, from the launch to the end of the mission life. Mission Operations also receive, process, and share payload data.

Ground Station Network receives and sends communication data via a physical link, leading them from the spacecraft to the control center and vice versa. It is composed by a ground network connected with one or more antennas, pointed towards the space object.

3.4 – LAYOUT FROM A SECURITY PERSPECTIVE

From a security point of view, a different division can be considered. The Transfer Segment can be split between the other two segments, considering the launch facility as a part of the Ground Segment, and the launcher as a temporary component of the Spacecraft.

According to CCSDS, two other components shall be considered to evaluate security: **Users** and **Communication Link** [12]. This different layout is represented in Figure 3.

Users represent people using the services provided by a satellite, and the human factor in the mission preparation and management. All these people have responsibilities and tasks that are of primary importance for the mission success.

Communication Link is the connection between the spacecraft and ground, with physical and logical layers. The most peculiar feature of a space system is the extremely long radio (or optical) link from Earth to Space.

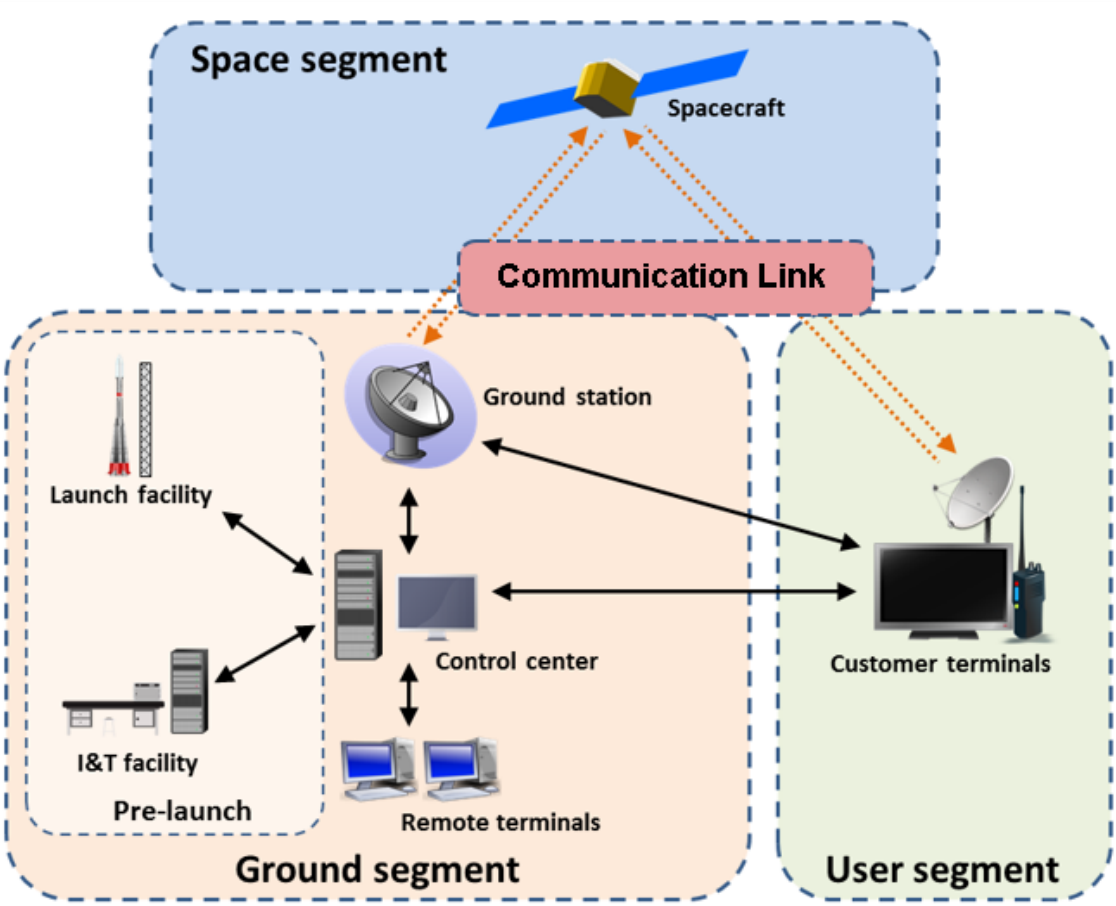

FIGURE 3 - SPACE LAYOUT FROM A SECURITY PERSPECTIVE [13].

3.5 – Security Threats Against Space Missions

Before producing a matrix for Space infrastructure, threats that are relevant for such a system have been considered, gathering knowledge from the related literature. Research has been carried out to collect and analyze the available knowledge.

According to CCSDS, a space mission can be exposed to a wide number of threats, that can be divided into active and passive threats [12].

When a threat source, like an APT, actively interferes with the attacked resource, the threat is called "active". Examples are jamming of a communication, gaining access to a communication channel, sending packets to command the resource or to mislead the owner, data damaging, modification or using malwares. The active threats are usually easier to detect, as they send packets or leave visible traces or damages.

If a threat source acts without an active interaction with the target, it is called "passive". Examples are interceptions of communication channels with a subsequent traffic analysis.

Threats can also be split according to the main components of space systems that can be targeted: Users; Ground and Control System; Communication Network; Space Elements. This division is depicted by CCSDS in Figure 4.

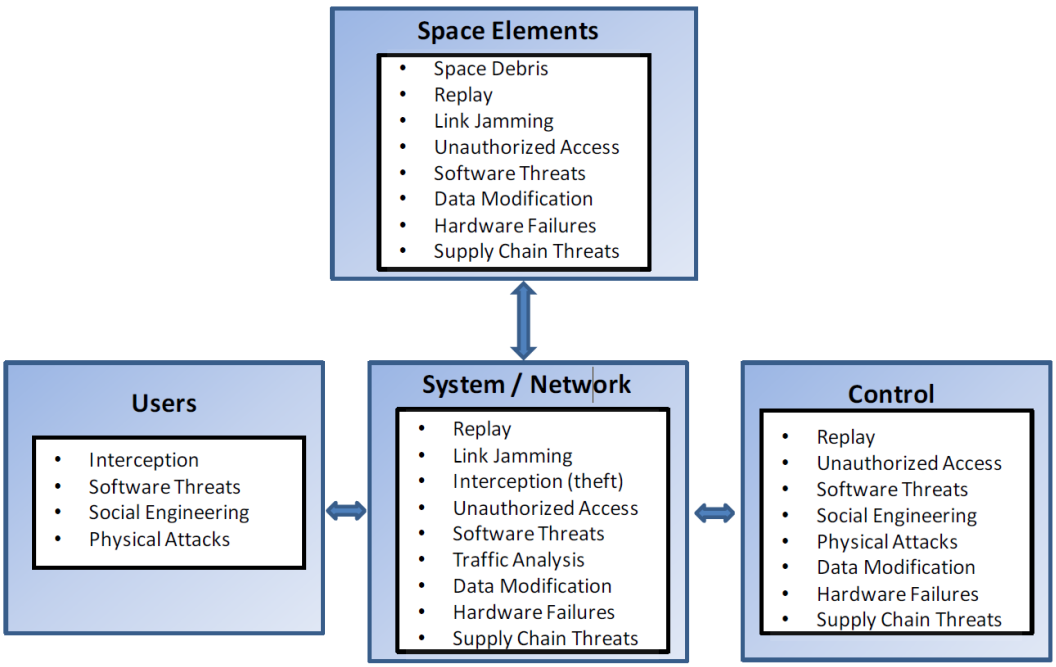

FIGURE 4 - POTENTIAL THREATS TO CCSDS SPACE MISSIONS [12].

If the human factor is considered, *Users* are exposed to similar threats than IT systems users, with attacks that aim to steal them confidential information and knowledge. These attacks can be interception of their communications, vulnerabilities, malicious features in the software they are using, social engineering attacks, or physical attacks that threaten human lives or force people to act in nasty ways.

The *Ground System* (in the previous figure it is referred to as Control) is based on terrestrial networks and devices, and it is exposed to threats that are comparable to the conventional IT threats, like software/hardware attacks, network analysis and access.

More important differences emerge when the latter two elements are considered, for which the classical cybersecurity approach does not provide sufficient coverage. For this reason, we focused our work mainly on this aspect.

The *Communication Network is* the link used to communicate with the spacecraft, that is characterized by distances that can be high or enormous (in case of deep space missions) and by a low power transmission, inversely proportional to the square of the distance, also due to the limited power available on the satellite. Communication Network is basically the only way to interact with the resource: if it is lost, the resource is lost. Consequently, it is exposed to every kind of radio-channel threat, and it is a valuable target for attackers.

The link can be jammed to prevent the communication, or it can be intercepted to access the data to steal or to perform a replay attack. If both the Tactics are used together, intercepting the communication while it is jammed on the receiver, the modification of the received data is also possible.

The network link can be targeted also internally, acting on hardware or software components. Communication hardware can be damaged by high power beams or compromised before the launch with a violation of the supply chain. An adversary can also interrupt the communication by modifying the on-board software or configuration.

All these threats were more difficult to deploy in the past, mainly because of the high communication distance, restricting the attack availability to countries or organizations with a high level of knowledge or capabilities. Today, with the increasing interest and diffusion of space infrastructures, this assumption is increasingly weak.

The last element, the *Space Element*, is the most valuable and exposed resource. As we said for the Communication Network, the main difference with a normal system is the high distance, that makes a physical repair - but also a physical attack - extremely difficult

and expensive. As a result, every kind of problem or violation, like unauthorized access or hardware failures, can be solved only remotely, and in case of unsuccessful intervention the resource loss is definitive. The supply chain threats are also dangerous, because of the almost impossible component substitution after the launch. A physical damage can come from space debris, that can be also caused on purpose. The Space Element can also be threatened by software and hardware attacks, depending on its specific characteristics. A summary is shown in Figure 5.

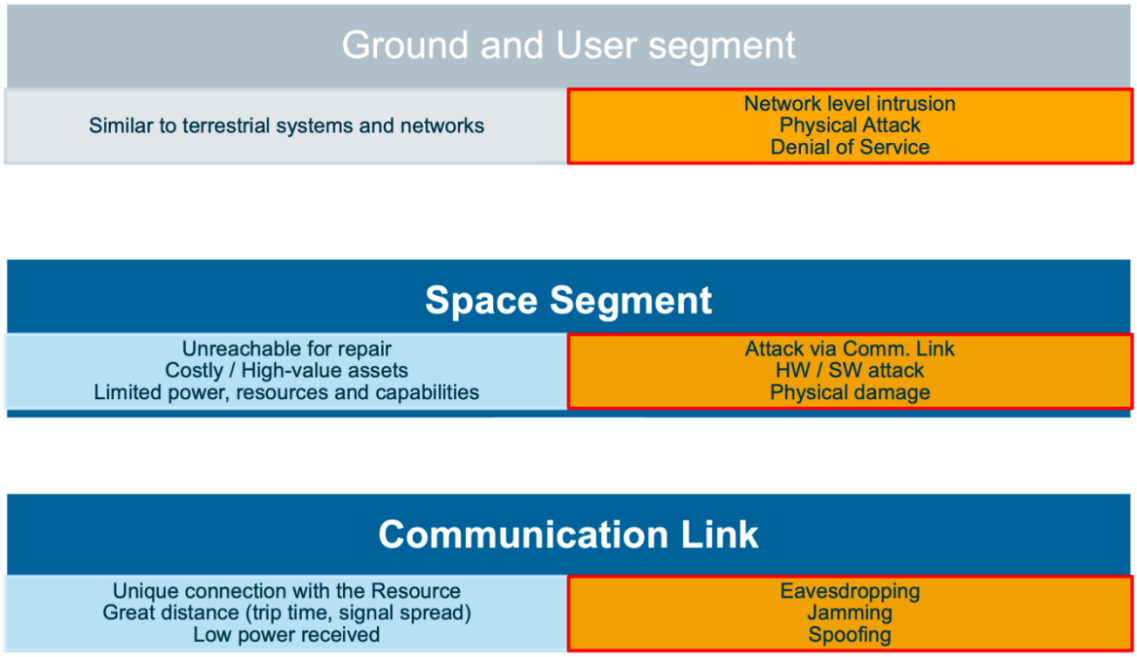

FIGURE 5 - SPACE SYSTEM SEGMENTS AND RELATED THREATS.

4 – DEFENDING A SPACE SEGMENT

4.1 – GROUND NETWORKS: THE MITRE ATT&CK FRAMEWORK

The Cyber Threat Intelligence on a space system needs a specific tool, tailored for it. The request of ESA was to realize a specific ATT&CK-like matrix to cover the threats that can target the Space environment. The existing Enterprise ATT&CK matrix [14] was chosen as starting point.

MITRE ATT&CK - abbreviation for Adversary Tactics, Techniques, and Common Knowledge - "is a globally accessible knowledgebase of adversary Tactics and techniques based on real-world observations" [1]. It exists since 2013, when it was developed to detail how APTs use Tactics, Techniques and Procedures to attack enterprise networks. All the possible attackers' behaviors come from analysis of security incidents already occurred, and their description is maintained broad and at high level [15].

ATT&CK can be used by organizations to assess their cyber risk, evaluating possible adversary behaviors during the various phases of an adversary attack lifecycle. Depending on company's assets and system's security gaps, defenders can study and prioritize Mitigations to put in place.

ATT&CK is built by Techniques and Tactics, structured in Matrices. The main elements are the Techniques, that represent actions that adversaries can perform to accomplish objectives and what they can gain with a specific action. Some of the Techniques are divided into sub-Techniques, to show in detail how each of them is executed.

The Techniques are related to one or more Tactics, that represent the tactical objective of the attacker, the reason why he executes the specific Technique. An attacker can implement sequences of Techniques to achieve a goal: these sequences are called Procedures [5].

ATT&CK also provides Mitigations to avoid or limit the success of Techniques, and detections used to be aware of an ongoing attack.

The relationship between Tactics, Techniques, and sub-Techniques can be visualized in the ATT&CK matrix, a table-like structure that shows all of them (see Figure 6).

The Tactics and Techniques are differentiated according to the considered system. To achieve this goal, more matrices have been developed [16]. The most relevant are the

Enterprise matrix, covering the action against an enterprise network (Windows, macOS, Linux, Cloud environments, etc.), the Mobile matrix, tailored for iOS and Android devices, and the ICS matrix, developed for industrial control systems and networks.

FIGURE 6 - MITRE ATT&CK MATRIX FOR ENTERPRISE (CROPPED) [1]

4.2 - THE NEED FOR A MATRIX FOR SPACE SEGMENT

The most similar extensive and generic MITRE matrix to the desired work result is the Enterprise matrix. It is structured in Tactics that describe well external adversaries attack procedure on computer information networks, but it fits only partially the Space Domain use case.

In analyzing the techniques, it is clear that a conspicuous part of them is not applicable in a space system. This is due to the particularities of this type of structure, which is extremely different from information systems and networks.

The Ground stations, with all their infrastructures, networks, and antennas, are today highly connected with ground networks and are exposed to many of the enterprise threats. The Enterprise matrix results useful to assess the security of the ground component.

The situation is completely different when the space component is considered. When the signal is transmitted over the radio channel, the security shall contemplate its peculiarities. The signal travels long distances and with a low power level, especially the downlink signal sent from the spacecraft, usually with energy constraints. The great travel distance also causes the signal to spread over a wide area on the ground. The radio communication results exposed to different kinds of adversary attacks: eavesdropping, jamming, spoofing, and so on.

The main difference with a terrestrial system is the position of the resource: a spacecraft is at a far distance, almost impossible to physically reach, and this limits the available threats.

Another difference is the on-board software, that is usually a real-time OS working as a control system. This excludes lots of techniques available on the ATT&CK matrix, developed for systems that are more complex and dynamic.

A further characteristic is the high economical value of the spacecraft, that cannot be protected against attacks aiming to physically damage it.

4.3 – METHODOLOGY

The result of the work is a Framework for Space Segment containing Tactics and Techniques, and the method chosen to compile it has been the selection of the applicable techniques from the ATT&CK Enterprise matrix, followed by the addition of Techniques and sub-Techniques relevant for the Space Segment. The focus of this research has been directed towards all the differences with classical IT systems, to include the threats that are missed by terrestrial frameworks.

To reach this goal, several documents concerning space security and threats have been studied, in addition to telecommunication standards from CCSDS [17] and ECSS [18]. The available documentation includes lots of threats, coming from different type of analysis and approaches. Furthermore, internal ESA knowledge has been used, leveraging on meetings with experts in various topics [19, 20, 21, 22, 23]. All the collected threats and information have been transformed into Techniques and sub-Techniques, accompanied by description and source references, and inserted in the ATT4S matrix. Some of the Techniques in the matrix come from events already occurred. However, it is worth noticing that most of them have not been applied yet, even though the technology already exists. For example, while ASAT weapons have been tested by various governments, nobody used them against other organizations so far.

This analysis has led to a wide view of the security condition of the Space Domain. The resulting matrix is a broad and general knowledge that aim to cover all the possible Space Systems and components, maintaining a high level of detail. A deeper detail to cover some specific missions, components or technologies is not part of this preliminary version.

In the following chapter, the outcome of the above methodology, which resulted in the proposed Framework for Space, is presented. Due to the high flexibility of the ATT&CK matrices, the same structure was used. The threats are organized and explained in Techniques, assigned to the same MITRE Tactics, that model in detail all the adversary phases. Although the adversary's tactical objectives remain the same as in normal systems, strong differences exist in the results that can be achieved. Furthermore, Techniques, the way attackers act to achieve those goals, are the items that change drastically from terrestrial systems.

5 – TACTICS AND TECHNIQUES

In this section, each subchapter corresponds to a Tactic, and for each Tactic all the corresponding Techniques are listed, explaining the characteristics of the sub-Techniques without listing them all.

All the Techniques that have been produced are underlined, while all Techniques without underline come from MITRE Enterprise matrix. In many cases, also MITRE Techniques have important differences when are applied to Space, which are explained in the description.

Since the Tactics are strictly connected, and every attack consists of many Tactics in an ordered chain of actions, the Techniques are also strictly related together. Many Techniques need the achievements of the previous ones as input, to continue with the following step.

5.1 - RECONNAISSANCE

As in ordinary networks and systems, before starting an attack, an adversary needs to know the victim's system, to better understand what he is going to face. A good awareness of a system permits to find which assets can be stolen, which services can be attacked and the amount of damage that can be caused.

The attacker tries to determine the structure of the system, discovering a weak point to initiate the attack. Furthermore, a successful attack usually exploits some vulnerabilities or flaws in the system structure, using them as an access point to get into the system. If defenses are in place, their knowledge is useful to avoid or to disable them.

All these requirements are included in the Reconnaissance Tactic. The different techniques are explained below:

PASSIVE INTERCEPTION (RF/OPTICAL)

An attacker tries to gain knowledge about which communication protocols are used and how, looking for manners to exploit them. A Spacecraft configuration, for example the Safe Mode, could be detected with this Technique. This accomplishment can be executed by intercepting, recording, and analyzing the signal to extract as much information as possible on the communication protocols. For example, different protocols

can apply SDLS security [24] to only part of the services, and this could be a relevant information.

The beam of an RF downlink signal sent by a far spacecraft is spread on a large ground area on the Earth, and the possible scanning area is wide. Receiving a satellite signal is simple and cheap, with general purpose SDR that can be used to record and demodulate transmissions. Various open-source projects exist, e.g., NyanSat.

Optical link can also be used for satellite feeder and intersatellite links, for some special payloads, or for deep space communications (availability problem caused by clouds should be considered if the receiver is on the Earth). On the other side, optical communication can be intercepted, unless secured by encryption algorithms.

ACTIVE SCANNING (RF/OPTICAL)

The technique is the same as the Passive Interception, the difference is that the attacker interferes with the Space Resource by actively sending signals/packets to it and/or to the GS, to activate the transmitter and to induce a reply. The scan can be similar to a brute force attack, aiming to guess the used frequencies and protocols to obtain a reply.

Both the Passive Interception and Active Scanning techniques can be divided in two sub-Techniques, depending on the target: the Telecommand (TC) channel, the Telemetry (TM) channel, or a mission specific channel.

GATHER VICTIM MISSION INFORMATION

An attacker tries to gather information about a specific mission to target it. An attacker can find information about firmware, software, hardware, frequencies, protocols, cryptographic algorithms used in a mission, and other knowledge like the spacecraft position and trajectory.

The application of this technique in the supply chain can lead to a software/tools/datasheets or a design leak. If COTS or open-source components are used, information can be easily gathered online or from the producing company.

GATHER VICTIM ORG INFORMATION

An attacker may collect information about the victim organization, and all the companies connected by common projects, supply contracts and business relationships.

“Useful information may include the names of divisions/departments, specifics of business operations, as well as identity, roles, and responsibilities of key employees” [14]. Information can be used to conduct phishing attacks, or to target people’s access and permissions to connected networks or resources.
Prime industry and subcontractors are useful for supply chain information, to plan a supply chain attack.

Victim's physical location can be used during targeting.

PHISHING FOR INFORMATION

“Adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt to trick targets into divulging information, frequently credentials or other actionable information” [14]. Gathering data from the victim is the final objective.

In a Space system, the attack may target Ground Segment operators in order to gain useful information to target the Ground Segment later.
The attack can also target Industries or Space Agencies that are involved in development, and it could result in information leakage. Stolen knowledge may be used to direct the attack towards a specific objective, or to develop hardware to affect supply chain.

SEARCH CLOSED SOURCES

Technical, organizational, or business information about victims can be purchased from reputable private sources and databases, or also less-reputable sources such as dark web or cybercrime black-markets.

SEARCH OPEN WEBSITES/DOMAINS

Adversary could search online information about the organization, using available websites or social media, to gain an initial knowledge on the victim. Information can be locations, involved people and their roles, etc.

IN ORBIT PROXIMITY INTELLIGENCE

The attacker, mainly a military organization, can use satellites positioned in proximity to the victim satellite to gather information, visual or radio, on the satellite capability or

on its work.

Proximity intelligence can be visual, with cameras or other optical sensors, to gain information about satellite's hardware, or electromagnetic, using antennas to intercept communications or to measure other EM emissions to attempt a side-channel attack.

5.2 - RESOURCE DEVELOPMENT

The attacker may need different resources to attack a system, and may purchase, find, produce, or steal them from the owner. The suitable resources can be files, like software, firmware, cryptographic key material, or description documents. All of these are useful to gain or to maintain the access to the system. The resources can also be hardware used to reach a space system, like Ground Stations or satellites, or to physically damage it, like space debris.

ACQUIRE OR BUILD INFRASTRUCTURE

An attacker can buy, steal, or build a Ground Segment, or he can easily request it if cloud based [25]. He can also launch a new satellite or gain control of an existing one. Antennas, lasers, or other equipment able to jam a radio or visible-light frequency can be useful to prevent communication or an image acquisition. These instruments can be fixed on ground, mounted on vehicles like trucks, ships, aircraft, or also installed on board of satellites.

COMPROMISE CREDENTIALS

Important credentials are cryptographic keys, but also cloud-based ground station's or other cloud services' credentials.

An attacker can also spoof credentials if the digital signature algorithm used by the CA is of insufficient cryptographic strength. Utilization of a weak cipher for carrying out protected simple authentication makes possible to reverse-engineer the original password.

COMPROMISE INFRASTRUCTURE

"Adversaries may compromise third-party infrastructure that can be used during targeting. Infrastructure solutions include physical or cloud servers, domains, and

third-party web and DNS services" [14] if the attack aims to hit the network part of a system, but also Space related facilities, like Ground Systems or Satellites.

If a Ground System is located in a remote area with limited physical security controls, a physical violation of the site is possible. Authentication systems should be implemented that make it difficult to use without proper authorization.

Compromised or malicious satellites might be abused by adversaries to achieve kinetic effects on other satellites in orbit, such as sensor interference or manipulation.

OBTAIN AND/OR DEVELOP CAPABILITIES

Adversaries may build, buy, or steal different capabilities to target a space system. They can work on cryptographic material used for authentication or signatures. X.509 certificates are recommended by CCSDS [26]. A risk for CCSDS systems utilizing credentials is that an attacker gains control of the credential-management system and issues credentials. If the credential management is compromised, existing credentials must be invalidated and all credentials reissued. Since the authenticity of an X.509 certificate depends on the digital signature of the CA attesting to the credential, if the digital signature algorithm used by the CA is of insufficient cryptographic strength, a credential can be forged.

Adversaries can find vulnerabilities related to commonly used or space-related software and protocols.

An attacker can guess the Spread Spectrum or the frequency hopping sequence, to reconstruct the received signal. The use of a cryptographic DSSS sequence can mitigate this problem.

An attacker can previously forge TC/TM commands and send them afterward to the system (including malformed TC/TM for flooding attacks) if authentication is not applied. As a mitigation, CCSDS SDLS protocol incorporates authentication through MAC.

Adversaries can obtain or create malicious capabilities inside hardware or software, intended to be used in a specific project. Injecting the malicious HW/SW in the right place is difficult, as is ensuring that the part will be integrated into a system.

An adversary can use ASAT weapons or a satellite collision to produce space debris, creating a threat for all the SVs in the related orbit.

An attacker can also develop or obtain software or hardware tools that can be used to attack a space system, e.g., to research and test vulnerabilities.

5.3 - INITIAL ACCESS

Accessing a system is the first step that an attacker performs against it, after the preparatory phase. He can use various techniques to gain the foothold in the system, and then to continue with his malicious operations.

The attacker can target the ground station or try to get into the space component. Due to the unreachability of this last component, initial access techniques are usually related to a physical access before the launch or to the violation of communication channels.

COMMUNICATION CHANNELS

An attacker can leverage communication channels to initially access a resource, using TT&C or a PDT channel, opening a communication link to compromise the victim system. An attacker can perform different actions.

An attacker can access data exchanged in a payload channel or in a TC/TM channel, decrypting them if encrypted, or simply accessing unencrypted data. Many satellites ISPs send sensitive customer traffic in clear text because of bandwidth/latency limits. As mitigation, communications can be encrypted and specific traffic protocols can be used. "The Space Data Link Security Protocol provides a security header and trailer along with associated procedures that may be used with the TM Space Data Link Protocol to provide data authentication and data confidentiality at the Data Link Layer" [24].

An attacker can send spoofed TC/TM packets by introducing a fake signal with erroneous information; this is particularly easy if the channel is unencrypted. Encryption is the best mitigation, together with the Space Data Link Security Protocol as in the paragraph above.

An attacker can exploit the TC channel if a spacecraft is in clear mode, e.g., during safe mode of operation.

An attacker can use brute force to gain access to a TC channel, to force encryption or to guess the valid commands.

An attacker can record and replay TC/TM packets to deceive the spacecraft or the ground station, causing an unexpected behavior or an erroneous evaluation of the

spacecraft status. Usually, the TM replay does not cause an impact, unless timing information are transmitted. CCSDS SDLS protocol incorporates anti-replay protection using incremental sequence numbers.

SUPPLY CHAIN COMPROMISE

In addition to normal supply chain threats, that are related to software, an attacker can replace firmware or hardware products in the supply chain with a custom or counterfeit part, to damage the system or to use it as a future backdoor.

An attacker can also induce the intentional use of a not genuine HW component to reduce the system reliability.

TRUSTED RELATIONSHIP

An attacker can compromise the system of a contractor company, to steal, modify or damage resources. A connected company or a research institution, scientific or not, can be compromised with the same objective. Connected networks or data exchanges can be leveraged to propagate the attack.

If the gateway is not controlled by the project agency or company, the admin has access to whatever is transmitted without encryption. The same problem exists if the gateway passes under the control of an attacker. To mitigate this, the Space Link Extension permits to transmit data without decrypting them up to the Mission Control System (MCS).

VALID CREDENTIALS

Adversaries may obtain and abuse credentials to gain Initial Access or Persistence in a space resource. Compromised credentials may be used to bypass access controls placed on systems within the network and to decrypt communication, to send authenticate messages and to take control of the spacecraft. Gained credentials may even be used for persistent access to the resource.

Adversaries may obtain and abuse master or session keys, or target the digital certificates used for the authentication.

GROUND SEGMENT COMPROMISE

Adversaries may compromise Ground Segment using it as a steppingstone to get Initial Access to the Space Segment and the system in general. Lots of existing attacks against a Space Resource need a communication, and a Ground Segment is needed. If an attacker comes into an authorized GS, it is a step closer to the compromission of the system. The compromission can be remote, producing a network access that can be leveraged to spread into the system. If a Ground System is located in a remote area with limited physical security controls, a physical violation of the site is possible. There are usually authentication systems that make it difficult to use the GS functionalities. The attacker can access the Ground Control Segment, to target satellite constellation control and management or switch off the payload functionalities, or the Ground Mission Segment, to target the specific mission objectives, or to interact with the payload.

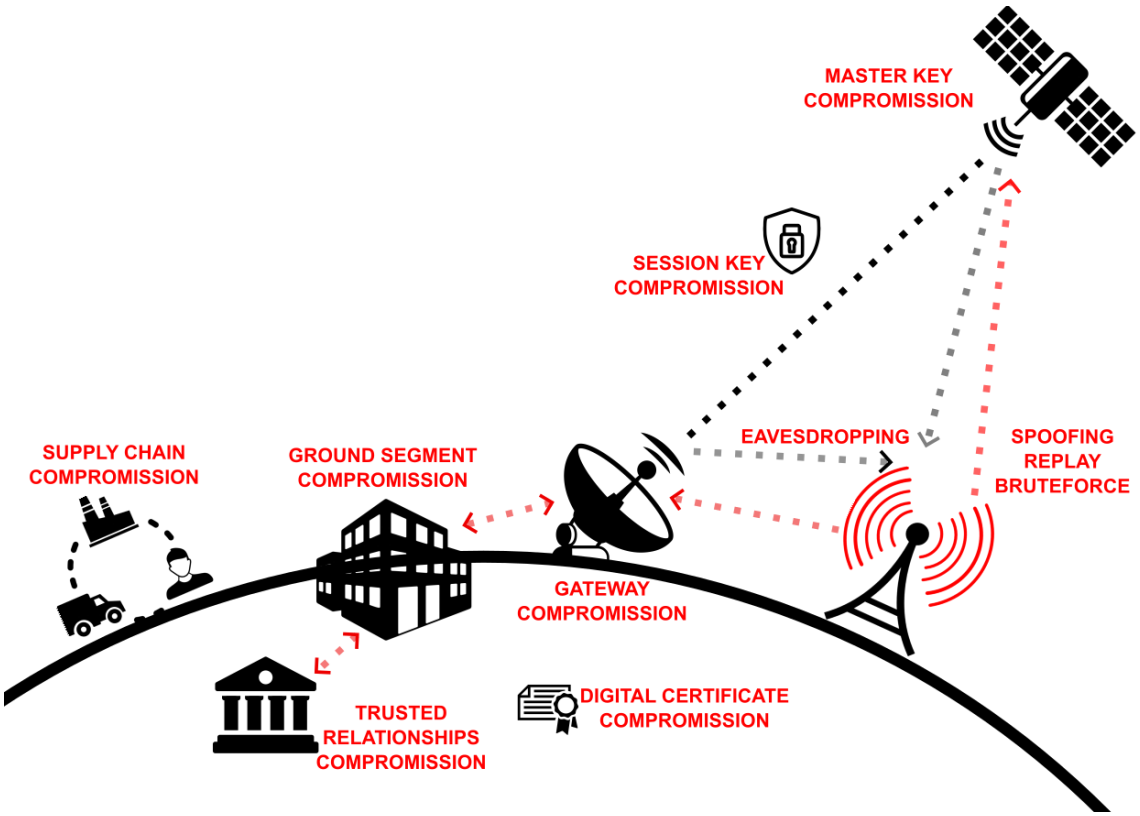

FIGURE 7 - OVERVIEW OF ALL INITIAL ACCESS TECHNIQUES.

5.4 - EXECUTION

All the techniques in the Execution Tactic are related to an adversary code running inside a machine. The code execution is usually used to accomplish other goals, like control the system or modify its parameters. In a space system, an attacker can use the gained access to the payload or to the TC system to interact with the spacecraft, attempting to modify the resource's behavior.

ON-BOARD CONTROL PROCEDURES MODIFICATION

An On-Board Control Procedure (OBCP) is a software program designed to be executed by an OBCP engine, which can be easily loaded, executed, and also replaced, on-board the spacecraft. An attacker can attempt to modify OBCPs to execute its own commands and control the spacecraft.

The attacker can modify OBCP gaining access to the command line interface of the OBC and interacting with it, exploiting MicroPython flaws or vulnerabilities or, in Unix-based OS (e.g., CubeSats) the Unix Shell can be used also to harm the system integrity.

HYPERVISOR PORTS BETWEEN PARTITIONS

An attacker who has control over a partition can use open ports between the partitions to overcome hypervisor's protections and damage another partition. This option is available for OS such as Xtratum, PikeOS, Air.

PAYLOAD EXPLOITATION TO EXECUTE COMMANDS

If an attacker gains access to the payload, he can execute TCs; in addition, he can propagate the attack exploiting payload activities.

NATIVE API

Operating systems like RTEMS provide API to interact with. An attacker can exploit them or abuse a vulnerability/misconfiguration to maliciously execute code or commands.

5.5 - PERSISTENCE

Persistence collects techniques used to maintain an undisclosed access to the resource over time, with the aim to act later, combining them with Defense Evasion techniques if needed. Persistence techniques consist in manipulation of the security components to permit a new access, or in preinserted or configured backdoors to permit a side access to the system.

KEY MANAGEMENT INFRASTRUCTURE MANIPULATION

Key infrastructures provide the technical means for managing the key life cycles as well as for the distribution of keys using security protocols or other means. If an attacker manipulates them, he can gain and maintain an authorized access to the protected resource. Encryption keys used to encrypt TM/TC can be replaced in order to gain permanent access to other functionalities, or to temporarily interrupt the owner's control.

VALID CREDENTIALS

The technique is the same as Initial Access Tactic. The attacker can use them to maintain an access to the resource.

BACKDOOR INSTALLATION

An attacker can interfere with the hardware or the software by integrating or modifying the existing software, hardware configuration, or the transponder configuration to allow future access to the resource.

The attacker can hardcode credentials during the supply chain phase with custom credentials, to have a secure access to the resource if the component is integrated in the system.

Replacement of a product in the supply chain with a custom or counterfeit part can be performed to damage the system or to use it as a future backdoor.

An attacker can modify the OBSW to permit a future access on the resource with a software backdoor.

An attacker can also modify the payload hardware, software, or configuration to create a future access on the payload itself, either to target it or to use it against the whole resource.

PRE-OS BOOT

"Adversaries may abuse Pre-OS Boot mechanisms as a way to establish persistence on a system" [14]. Adversaries can overwrite boot data modifying or replacing components before the launch or updating them later if an update capability is implemented. Detection is very difficult, because defenses are usually working at higher levels.

Persistence at a pre-OS level can be gained by modifying the firmware in a resource. System firmware is quite static and usually does not provide detection capabilities. A firmware level manipulation can remain unnoticed until the later phases of the attack.

5.6 - PRIVILEGE ESCALATION

"Privilege Escalation consists of techniques that adversaries use to gain higher-level permissions on a system or network" [14]. In a limited system as the Space System is, examples are the overcoming of hypervisor's limits and controls, or the abuse of bus's hierarchy.

ESCAPE TO HOST

If containers or hypervisors are used, an attacker could overcome the container fences and gain access to the host system. Separations between applications may be defeated, and malicious operations could affect other functionalities. This attack can leverage common utilities, schedulers, shared memory, or vulnerabilities.

"Gaining access to the host may provide the adversary with the opportunity to achieve follow-on objectives, such as establishing persistence, moving laterally within the environment, or setting up a command and control channel on the host" [14].

BECOME AVIONICS BUS MASTER

An attacker can use a compromised device connected to an Avionics Bus to interact with the communication line and force the election to become the Bus master. This role can be used to disrupt the communication between other nodes.

5.7 - DEFENSE EVASION

Attackers can have more time to complete or to postpone the attack, or they can extend the attack duration if the resource owner does not discover it. If defense or detection systems are in place, they can attempt to disable or to avoid them.

IMPAIR DEFENSES

"Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior" [14].

A possible sub-technique is the triggering of the clear mode, via TC or consuming spacecraft resources, to disable or limit the security level of the spacecraft.

INDICATOR REMOVAL ON HOST

If a log is available, an attacker can delete logging onboard the spacecraft to hide illegitimate operations. A TC log service is usually not implemented on the spacecraft, due to resource constraints.

5.8 - CREDENTIAL ACCESS

A possible adversary goal is the credentials discovery, useful to have a hidden and stable access to the resource. Keys can be gathered by corrupting a weak security protocol used in a communication or compromising the key management facility or its communications.

RETRIEVE TT&C MASTER/SESSION KEYS

The attacker gains knowledge of a Session or Master Key. In general, there is no immediate way to discover this corruption before it is used to modify the system behavior.

There are multiple ways to gain keys. An attacker can gain control of the Credential-Management System and issues credentials, or he can also gain knowledge of a Session or Master Key corrupting the cryptographic algorithm.

The attacker can intercept messages that are transmitted as part of the Key Management Services with the intention either to obtain knowledge of a specific key or

to interfere with the Key Management Service. The CCSDS Recommended Practice provides specific means for protection of the OTAR key management service. However, it is assumed that all key management communication is protected by a security protocol such as the Space Data-Link Layer Security Protocol.

In case of a suspicious key corruption, the key replacement shall be executed as soon as possible. If the compromission is at KMS, there is the need to invalidate existing credentials and reissue all credentials.

5.9 - DISCOVERY

Discovery Tactic gathers all knowledge an adversary can gather about the system structure, implementation, or configuration.

The objective of this phases is to probe the environment for which an access is available, looking for other assets to attack.

KEY MANAGEMENT POLICY DISCOVERY

Adversaries may try to gather information about the implemented Key Management Policy.

"Security Policies are rules and regulations that describe the operational procedures required for proper key management. This includes the specification of rules for processes such as generation, distribution, and allowed use for cryptographic keys" [27].

TRUST RELATIONSHIPS DISCOVERY

Adversaries may try to gather information about Trust Relationships with other companies or organizations.

SYSTEM SERVICES DISCOVERY

An attacker can try to discover services running on board and gather information on them.

SPACECRAFT'S COMPONENTS DISCOVERY

Adversaries may try to gather information about Components of the Spacecraft, monitoring internal communication, actively communicating with the system, or from internal registries or configurations.

5.10 - LATERAL MOVEMENT

Lateral Movement Tactic is related to the access of another system or sub-system connected to a compromised component, leveraging a lack or a misconfiguration of separation tools. The attack can propagate to that component, delivering a wider access to the attacker.

LATERAL MOVEMENT VIA COMMON AVIONICS BUS

This attack is performed against a part of the system via a physical bus shared with a compromised system. An unprotected bus can be used to extend an attack to uncompromised components. For example, if payload has access to main 1553 bus, a hosted payload attack is possible. Fault injection or MiTM can be done into the 1553 bus. CANBus, SpaceWire, SpaceFibre, or other types of bus might be abused if detection and protection systems are not included in the protocol.

COMPROMISE OF ANOTHER PARTITION IN TIME AND SPACE PARTITIONING OS OR OTHER TYPES OF SATELLITE HYPERVISORS

If the payload is compromised, access to a critical partition can be gained through ports allowed by hypervisor. Information security is usually configured at the application level, with the execution confined to the application's partition and controlled communication with the remaining partitions. Time and Space Partitioning or other satellite hypervisor types should protect the system from interferences. All communication passes through the security components, which can include monitoring and cryptographic mechanisms.

5.11 - COLLECTION

An adversary who compromised the space resource or the communication channel can leverage his access to collect data. If the communication is unencrypted, the collection corresponds to the channel eavesdropping.

ADVERSARY-IN-THE-MIDDLE

"Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique" [14].

If unauthenticated gateways or unauthenticated interplanetary nodes are used, an adversary can substitute them with an own resource to collect or modify transmitted data. A satellite with stolen credentials can take place into a dynamic constellation and collect data.

DATA FROM LINK EAVESDROPPING

Adversaries can collect data transmitted over a channel if he is able to decode and decrypt the intercepted communication.

An attacker can collect and have access to data transmitted by TT&C if the communication does not rely on encryption. CSDS SDLS protocol incorporates confidentiality services through encryption of the frame data, that can be used as a mitigation.

Adversaries can collect data transmitted over the payload channel if it is used. Adversaries can also intercept range data to locate and more accurately target the victim spacecraft. Mitigation comes from higher level protocols, with encryption to assure confidentiality.

5.12 - COMMAND AND CONTROL

If the attacker has the system under its control, he can interact with it to command it. The TC channel is used to communicate with the spacecraft, sending spoofed command messages or delaying original packets.

TELECOMMAND

The attacker exploits an unencrypted channel or gained keys to send TCs to a spacecraft. He can send a Packet Utilization Standard (PUS) command to execute or schedule an action. The transmission of a TC can be scheduled on the Ground Station.

An attacker can use the TC channel by attempting to modify OBCP, to execute his own commands and control the spacecraft.

An attacker can upload a malicious code while the resource is out of connection with a

ground station. An attacker who wants to change the software image by uploading it needs more than one pass over the ground (LEO or MEO), due to the bandwidth/spacecraft speed ratio.

TC/TM DELAY

Messages can be registered while denied with jamming, then replied later, including the authentication tag. Usually, there is not an impact on the system because the TCs are not real time. This can become a problem if the transmitted timing is used for navigation. The TC counter does not detect this type of attack.

5.13 - EXFILTRATION

Exfiltration techniques are used to send data out of the resource through a communication channel, to steal them. The two common download channels are the TM and the payload channel. Both are radio channels with a broad diffusion on the Earth surface (due to the high distance), this results in an easy detection of the exfiltration, because the official GS can receive the "unexpected" packets.

EXFILTRATION OVER PAYLOAD CHANNEL

Malicious software can send data through the Payload channel (if implemented).

EXFILTRATION OVER TM CHANNEL

Malicious software can send data through the TM channel (usually the only connection channel available), inserting the data to be exfiltrated in the Transfer Frame Data Field of the TM Transfer Frame.

SIDE-CHANNEL EXFILTRATION

An adversary can exfiltrate data with a side-channel attack. This type of attack tries to extract useful information on cryptographic materials analyzing the physical behavior of a component. Timing of CPU operations can be leveraged to guess if a specific bit is set, if the execution of some line of code depends on its value. Power consumption, electromagnetic and acoustic emissions may also reveal information on the cryptographic key.

RF MODIFICATION

An adversary can exfiltrate data by modifying the RF components to send data with a different timing (and location), or with different frequencies. Antenna arrays can be used to send data into different beams.

OPTICAL LINK MODIFICATION

An adversary can exfiltrate data by modifying the optical communication components to send data with a different timing (and location).

5.14 - IMPACT

The adversary is trying to damage the system security, interrupting its normal execution, or damaging it physically. Due to the impossibility to reach the resource and repair/reprogram it, if the damage is too severe the resource is definitively lost. The damage can be at data level, targeting the stored or transmitted data, deleting them, or modifying them to deceive the receiver. It can be also at service level, interrupting a payload execution or hitting the communication with jamming and flooding to prevent it. Damage can be also at hardware level, destroying the space resource with electromagnetic power, kinetic weapons, or malicious hardware preinserted in the system.

RUNTIME DATA MANIPULATION

An attacker can use a controlled payload software or component to manipulate data in the same or in another component during the execution, if a MMU or a MPU is not implemented or is misconfigured. MMU and MPU are the best mitigations, but only the most recent space qualified microprocessors (LEONII/III) have a MMU available, that provides only write protection. For secure spacecraft avionics, protection against read/write and execution access is necessary. The MMU or a MPU is extremely important if the payload is not trusted.

TRANSMITTED DATA MANIPULATION

An attacker can modify transmitted data, jamming or overpowering the original signal and retransmitting a modified copy to the receiver, to command a spacecraft or to lead the system owner to erroneous decision.

An attacker can target the TCs sent from a GS, to change the spacecraft behavior, or he can tamper the TM sent from a spacecraft to change the GS received data. Intercepted and modified range measurement sent to the control center could lead to erroneous range measurements, which could cause incorrect trajectory determination. Mitigations are redundancy/diversity to protect the source and authentication to protect the message. To protect the data source, a star sensor offers a high level of reliability.
An attacker can also target the payload data sent from or to a spacecraft. To mitigate this, Navigation Message Authentication (NMA) uses symmetric/asymmetric key encryption to provide authenticity and integrity of the navigation data to the receiver.

DENIAL OF SERVICE

An attacker can perform a Denial of Service (DoS) attack to limit or block the service availability in a resource, between resources or between users. Politically motivated incidents were usually carried out through RF jamming or signal hijacking.
Spread spectrum signal has various advantages, but it can be susceptible to the near-far problem, where a malicious transmitter closer than the legitimate one or with higher data rate and power, located in space or on ground, can cause a higher power flux density on the receiver and a false PN lock. This can lead to jamming or spoofing of the original signal.

An attacker can exploit various sub-techniques to obtain DoS:

- In a network constellation without an efficient routing protocol, a network attack aiming to flood the network is possible, causing a saturation of an intersatellite link. This kind of attack can be executed by authorized users, intentionally or not (botnet malware on user devices).
- An attacker can jam the RF communication to prevent data being delivered. Waiting and communicating later is usually possible without noticeable problems in TT&C. Regarding short-range communications at a far distance from Earth, as between an orbiter and a lander in planetary missions with the use of Proximity-1 Protocol, jamming becomes difficult. Jamming of the uplink signal, from the lander to the spacecraft is difficult because of the interplanetary distance from the jammer to the receiver; jamming of the downlink transmission from the orbiter to the lander, which rely on terrestrial commercial frequencies, would result in the disruption of many other terrestrial links.

Jamming of the ranging signal could lead to the total loss of ranging data, and potential navigation errors. The C&S Sublayer provides methods for frame re-synchronization. Protection must be accomplished by physical-layer techniques such as spread spectrum and/or frequency hopping.

- An attacker can conduct optical attacks with high power laser beams to target optical sensors or optical links.
- If the victim uses a free space (over the air) communication, it can be threatened by jamming attacks.
- If the payload uses cameras or other optical sensors to take pictures or measurements, they can be blinded or damaged.
- An attacker can try to flood the spacecraft receiver sending great amount of data, valid or not. Since the Ground Station notices the status of the receiver, the power of the transmitter should increase to unlock the receiver from the messages flood, rising the receiver's threshold and cutting out the malicious signal.
- The lock of the spacecraft receiver or of the ground station with a continuous wave or with the obtained DSSS sequence can be a threat. Increasing the power is the only way to unlock the receiver, or it is unlocked when the spacecraft moves out of the LoS with the attacker GS. The attack depends on the receiver and system dynamics, that causes the doppler effect and requires a larger bandwidth. A possible mitigation is the use of a cryptographic DSSS sequence.
- If SDRs or digital signal processing software are used to provide radio functionality, insufficient checks in radio frame processing, coupled with malformed data packets, could lead to buffer overflows, and create denial-of-service conditions. This type of jamming is significantly stealthier as it is triggered by sending a small number of packets and does not require a continuous RF jamming signal.

TEMPORARY LOSS OF SATELLITE TELECOMMAND

Adversaries can replace encryption keys used to encrypt TT&C in order to gain permanent access to other functionalities, or to temporarily interrupt the owner's control.

PERMANENT LOSS OF SATELLITE TELECOMMAND

Adversaries can replace session and master keys in a space resource, to gain permanent access to the resource and permanently prevent the owner access. This attack leads to a definitive loss of the resource.

RESOURCE HIJACKING

An attacker can hijack resources of the space vehicle using them for different purposes. The attacker can target satellites with energy or resource constraints to induce them to prioritize power saving efforts and disable security controls. The satellite becomes then more vulnerable to other attacks such as gaining unauthorized access or eavesdropping cleartext communications. This goal can be reached with a regenerative payload "flooding", sending to the satellite more packets than expected to rapidly consume its energy. The exploitation of a payload application can achieve a similar result. The attacker can abuse the satellite bandwidth for the retransmission of own content. The attacker can maliciously consume satellite propellant resources to achieve the goal of reducing the satellite life.
The trajectory of a Space Resource can be changed to waste its resources, to prevent the Resource from doing its purpose, to create an irrecoverable damage or to use the resource for malicious actions.

SERVICE STOP

An attacker can interrupt services, disabling them or taking control over them. The ground facility can be disabled, or an attacker can take control of it with a cyber or physical attack. The loss of the GS can be also caused by environmental factors, uncontrolled or induced (e.g., fire).
An attacker can disable the payload, or parts of it, leveraging TC switch on-off commands. In a mission with a direct link to the payload, the latter can be disabled, compromising its command channel. Protect TC commands is needful to mitigate the threat.

RESOURCE DAMAGE

An attacker can attempt to damage a space resource, to cause a mission loss, in different ways:

- A space resource can be damaged if a counterfeit HW component breaks out.
- A space resource can be damaged if a specific HW component, built to fail after a specific period, breaks out. This is particularly relevant for ASIC and FPGA.
- An attacker can damage a receiver using a laser source for an optical receiver or an RF source for an antenna receiver. Physical damage of an RF part is extremely difficult, because of protections; still, it may be possible by using another satellite in near orbit.
- A space resource is damaged or destroyed if an impact with space debris happens. Space debris can be produced to harm resources in specific trajectories.
- An attacker can physically damage a satellite, with harmful commands or by attacking it with another vehicle. Heaters and flow valves of the propulsion subsystem can be moved. Proximity operations with other satellites are possible (kinetic kill vehicles, radiofrequency jammers, lasers, chemical sprayers, high-power microwaves, and robotic mechanisms). Other possible attacks are against critical software subsystems or internal timers.
- Attackers can use anti-satellite (ASAT) missiles, or other kinetic energy threats, to attack a resource from the ground or from a plane, without the need for an orbit insertion. Peculiarities of counterspace weapons are the easy attribution of the attack fault using missile tracking systems, and the generation of space debris. These systems could include payloads such as kinetic kill vehicles, radiofrequency jammers, lasers, chemical sprayers, high-power microwaves, and robotic mechanisms. The latter technology is developed to repair satellites or to remove space debris, but its use can be malicious.

  A nuclear explosion can also be used against all the space segments.
- Adversaries can command the satellite to collide with other satellites. This results not only in the loss of the resource, but also in a damage to another resource.

6 - MITIGATIONS

The Techniques presented so far represent actions that can be carried out by an adversary, with the final intention of fulfilling his attack. On the other side, defenders have options to block or limit the attacker's Techniques and protect the owned system from malevolent activities.

According to MITRE, "Mitigations represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed" [1].

Mitigations shall be evaluated, selected, and put in place to reduce the overall risk of threats, mainly against APT [28]. An accurate work must be carried out in the Risk Mitigation phase, resulting in a selection of mitigations to be implemented [3]. The peculiarity of the asset to be defended, the feasibility and the cost of the specific countermeasure, its effectiveness compared to the initial risk are selection criteria.

As well as the attacking Techniques, Mitigations are abundantly different in the Space environment. Although part of them derives from Enterprise systems, and are not listed in this thesis, numerous Mitigations are specific and additional. Different Mitigations have been gathered in bibliography, and a brief description of the Space specific is provided for each of them in this chapter. The relationships between them and the addressed Techniques are on the produced Excel matrix and on the website.

QUANTUM KEY DISTRIBUTION

Quantum Key Distribution is a technology that can be used to securely exchange symmetric encryption keys, leveraging properties of quantum physics. If an eavesdropper observes the communication, a perturbation in the transmitted photons is caused and the legitimate user can detect it. QKD is a controversial topic of research and investments, with a high theoretical potential and a high cost and complexity.

AUTHENTICATION

Authentication permits a secure access to the resource, verifying the actor's identity. It also protects a command or a message from spoofing or modifications. CCSDS SDLS protocol incorporates authentication through MAC. Authentication protects from attacks

aiming to access unauthorized resources, to spoof legitimate users, or to manipulate data and communications.

ENCRYPTION OF COMMUNICATIONS

Encryption of communications hides the message content to unauthorized eavesdropper, ensuring confidentiality. Moreover, it permits to ensure authentication and non-repudiation of the communication.

The Space Data Link Security Protocol provides a security header and trailer along with associated procedures that may be used with the TM Space Data Link Protocol to provide data authentication and data confidentiality at the Data Link Layer through encryption of the frame data. Payload traffic, if related to network communications, can use specific traffic protocols. Range data shall be encrypted, too.

The CCSDS recommended confidentiality algorithm is AES [29] using the counter mode of operation [30]. This algorithm operation mode permits a meeting point between a high security level and a good efficiency, by using parallelization.

If authenticated encryption is required, the recommended operation mode is AES/GCM [31].

CCSDS SDLS SEQUENCE NUMBERS

CCSDS SDLS protocol incorporates anti-replay protection with incremental sequence numbers. Increased sequence numbers can also permit the detection of unauthorized messages sent to the Resource.

SPACE LINK EXTENSION

The Space Link Extension permits to transmit encrypted data end to end without decrypting them at intermediated steps. This feature permits to keep data safe up to the MCS if the communication link runs across untrusted nodes or ground network.

PROTECT OTAR KEY MANAGEMENT SERVICE

Over-the-air rekeying (OTAR) is the process of updating encryption keys via an existing encrypted communication channel.

CCSDS Recommended Practice provides specific means for protection of the OTAR key

management service. All key management communication must be protected by a security protocol such as the Space Data-Link Layer Security Protocol.

PARTITIONING/SEPARATION

Time and Space Partitioning or other satellite hypervisor types should protect systems from mutual interferences, creating security borders between services and preventing unauthorized interactions.

MMU AND MPU

For secure spacecraft avionics, protection against read/write and execution access is necessary. The MMU or a MPU provide it and this is extremely important if the payload is not trusted.

REDUNDANCY

Redundancy can improve the reliability and availability of a system, a data source, a service or a resource from faults and interruptions, either accidental or produced, or from deceiving attempts.
It consists in the inclusion of extra components, either hardware or software, which are not strictly necessary to functioning, but that start when other components fail. As a downside, it increases the cost and complexity of a system design.

DIVERSITY

Diversity can protect a data source from faults or deceiving attempts. Different components or software are less likely to break or have the same vulnerabilities, and a compromise of one of them does not automatically become a compromise of the whole system. Different locations are exposed to different physical problems.

STAR TRACKER

A star tracker is an instrument enabling accurate and autonomous control of a satellite's attitude, by analyzing the placement of the surrounding stars. The estimation is reliable and extremely difficult to spoof.

NAVIGATION MESSAGE AUTHENTICATION (NMA)

For GNSS data, Navigation Message Authentication (NMA) uses symmetric/asymmetric key encryption to provide authenticity and integrity of the navigation data to the receiver.

CCSDS CODING & SYNCHRONIZATION SUBLAYER

In case of congestion or disruption of the link, the Coding & Synchronization sublayer provides methods for frame re-synchronization for TC, TM, Proximity. The synchronization of the receiver with the data stream is initiated by the Acquisition Sequence, a preamble characterized by a high transition density bit pattern to support the initial symbol synchronization. The synchronization is maintained during the communication by the Communications Link Transmission Unit (CLTU), which consists of a Start Sequence as synchronization pattern transmitted at the beginning of the data frame, and an optional Tail Sequence after it.

A Pseudo-Randomizer is used to ensure sufficient randomness in the transmitted frame, to help synchronization.

SECURE SAFE MODE

In case of system problems, the Resource may enter in Safe mode, where the security functions are deactivated or bypassed. The system must have a fallback set of master keys to use in this case, to securely re-enable security functions and upload new sets of Traffic Protection Keys.

SPREAD SPECTRUM

Spread Spectrum is a system to spread the signal power over a large frequency band, hiding the signal itself and protecting it. Reconstruction of the original signal requires knowledge of the spreading sequence. The resulting signal is more difficult to find and intercept, to jam or to spoof.

CRYPTOGRAPHIC DSSS SEQUENCE

Spread Spectrum is a system to spread the signal power over a large frequency band, hiding the signal itself and protecting it. Reconstructing the original signal needs the

knowledge of the spreading sequence. The resulting signal is more difficult to find and intercept, to jam or to spoof. If the DSSS sequence is protected by a cryptographic sequence, a cryptographic key is needed to predict the spreading sequence's behavior.

FREQUENCY HOPPING

Frequency Hopping is a system to regularly change the carrier frequency according to a specific pattern. This procedure makes interception more difficult and protects the signal from interference, either deliberated or not.

MONITORING

Monitoring of the system state is fundamental to early detect undesirable behaviors or interactions. In case of Denial-of-Service attacks, the Ground Station should be able to detect the status of the receiver. If the receiver is targeted by attacks, the power of the transmitter should be increased, rising the receiver's threshold level, and cutting out the malicious signals.
Radio channel monitoring permits the identification of messages sent by unauthorized users towards the spacecraft. Internal system monitoring may discover malicious or erroneous operations.

NON-REPUDIATION MECHANISMS

Use mechanisms, like Digital Signatures, to ensure that nobody can deny responsibility for performing actions, communications or the origin of data.

DATA INTEGRITY SCHEMES

Use data integrity schemes to protect data from unauthorized modifications, or from unintentional corruptions due to noise or storage defects (hashing, check values, digital signatures).
SDLS provides integrity protection on the transmitted data, with the computation of a MAC.

RESILIENCE

Resilient hardware (e.g., SOS) protects systems, facilities, services, or data from damage or from Service interruption attacks.

PHYSICAL SECURITY

Guards, gates, and other physical security countermeasures, permit to defend facilities from undesirable accesses, sabotages, or damages made on purpose.

ACCESS CONTROL

Access control systems authenticate users and enforce authorization, avoiding that attackers or unauthorized users reach unpermitted services and resources, modify system configurations, and take control of them.
Access control is needed to identify actors who try to interact with the system, or take place in a network, and it defines if they are authorized or not.
The installation of backdoors in the system, and the exfiltration of data from it can be prevented or at least made more difficult if an access control is implemented. Furthermore, access control can protect from alteration of system settings, disablement of defenses, or from the deletion of logs. Without the access control, the attacker could take control of the asset, abusing the resources, misconfiguring OBCP to hijack or damage it, he can interrupt the provided services or also take possession of the spacecraft, changing the cryptographic keys.

TIMESTAMP

Timestamps can prove when a message has been written, protecting it from a delay or a replay attack.

SUPPLY CHAIN CONFIDENCE

Supply chain confidence is fundamental to mitigate risks or attacks related to supply chain, as introduction of backdoors or malicious capabilities in components that are going to be integrated in the system. Knowledge of the product chain, either hardware or software, reassurance in the measurements, tests, inspections, and certifications, can limit possible attack vectors and threats.

AUTHORIZATION

Authorization mechanisms protect functionalities from being executed by unauthorized entities.
Authorization can avoid the exploitation of TCs, API, CLI or other command methods to modify system configuration. Backdoor installation, data manipulation, and the use of Payload and Spacecraft's resource are limited if authorization is applied.

ACCOUNTABILITY OF ACTIONS

Every access or action shall be accounted to a user, entity, or organization, to keep track of roles or to attribute the responsibility in case of problems.

AUTONOMY

Autonomy can protect against denial-of-service attacks, mainly targeting the TT&C link, maintaining the system at work during absence of commands.

TRACK DEBRIS AND SPACE VEHICLES

Tracking of space elements brings consciousness about dangerous Space Debris that can cause collision. Knowledge of position and trajectory of other satellites, in addition to their owner, purpose and implemented technologies, permits to be aware of malicious neighbors.

7 - THE ATT4S MATRIX FOR SPACE

All the identified adversaries Techniques and sub-Techniques have been organized in an ATT&CK-like matrix. Each of them has a description explaining how an attacker can use it, and which kind of asset he could target. Furthermore, sources for the Techniques are provided in the Excel file and in the website Techniques pages; also, if applicable, references to related protocol standards or recommendations are provided.

All the Techniques are assigned to one (ore sometimes more than one) Tactic, each of which is represented in a column; the column can be divided in two, with the Techniques on the left side and, if any, the sub-Techniques on the right side.

The resulting ATT4S matrix is shown in Figures from 8 to 14, in the shape of a table, for convenience split in various figures with two Tactics for each, that should be placed side by side to reconstruct the whole matrix.

The Techniques and sub-Techniques written in black are those in common with the ATT&CK matrix, while the new components of ATT4S are written in blue.

Reconnaissance		Resource Development	
Active Scanning (RF/Optical)	Mission specific channel scanning	**Acquire or Build Infrastructure**	Ground segment
	Telecommand Protocol Scanning		Jamming equipment
	Telemetry Protocol Scanning		Satellite
Gather Victim Mission Information	Cryptographic algorithms	**Compromise Credentials**	Compromised Services Account
	Firmware		Compromised Cryptographic Keys
	Frequencies	**Compromise Infrastructure**	Ground Segment
	Hardware		Satellite
	Other mission specific information	**Obtain and/or Develop Capabilities**	Code Signing Certificates
	Position/Trajectory		Digital Certificates
	Protocol specifications		DSSS code or Frequency hopping sequence
	Software		Malicious supply chain capabilities
Gather Victim Org Information	Business Relationships		Software vulnerabilities
	Determine Physical Locations		Space Debris production
	Identify involved industries and other organisations		Space Protocol Vulnerabilities
	Identify Roles		Tools for attacking space systems
Passive Interception (RF/Optical)	Mission specific Channel Interception		
	Telecommand Protocol Interception		
	Telemetry Protocol Interception		
	Safe Mode Indication		
Phishing for Information	Spear Phishing to Ground Segment Operators		
	Spear Phishing to Industry/Space Agencies		
Search Closed Sources	Purchase Technical Data		
Search Open Websites/Domains	Social Media		
In orbit proximity intelligence	Optical (visual) reconnaissance		
	Electromagnetic reconnaissance		

FIGURE 8 - PART 1/7 OF THE ATT4S MATRIX IN EXCEL FORMAT.

Initial Access		Execution	
Communication channels	Payload eavesdropping	Hypervisor Ports between partitions	
	TC Brute forcing	Native API	
	TC while in safe/clear mode	On Board Control Procedures modification	OBCP CLI
	TC/TM eavesdropping		Python - Micropython
	TC/TM Replay		Unix Shell
	TC/TM Spoofing	Payload Exploitation to Execute Commands	
Supply Chain Compromise	Compromise Hardware Supply Chain		
	Compromise Software Dependencies and Development Tools		
	Compromise Software Supply Chain		
	Compromise Firmware Suppy Chain		
Trusted Relationship	Compromise a contractor's or a scientific connected system		
	Gateway		
	Trusted Relationship via Federated Operations		
Valid Credentials	Digital Certificates		
	Master/session keys		
Ground Segment Compromise	Ground Mission Segment Compromise		
	Ground Control Segment Compromise		

FIGURE 9 - PART 2/7 OF THE ATT4S MATRIX IN EXCEL FORMAT.

Persistence		Privilege Escalation
Backdoor Installation	Hardcoded credentials and/or keys	Escape to Host
	Integration of custom malicious hardware	Become Avionics Bus Master
	OBSW modification	
	Transponder reconfiguration	
	Payload modification	
Key Management Infrastructure Manipulation	Replace session keys	
Valid Credentials	Master/session keys	
	Digital Certificates	
Pre-OS Boot	System Firmware	

FIGURE 10 - PART 3/7 OF THE ATT4S MATRIX IN EXCEL FORMAT.

Defense Evasion		Credential Access	
Impair Defenses	Triggering the clear mode	Retrieve TT&C master/session keys	Compromission of Key Management Facility
Indicator Removal on Host	Clear Command History		Cryptographic Key Corruption
Masquerading			Interception of Key Management Communication

FIGURE 11 - PART 4/7 OF THE ATT4S MATRIX IN EXCEL FORMAT.

Discovery	Lateral Movement
Key Management Policy Discovery	Compromise of another partition in Time and Space Partitioning OS or other types of satellite hypervisors
Trust Relationships Discovery	Lateral Movement via common Avionics Bus
System Service Discovery	
Spacecraft's Components Discovery	

FIGURE 12 - PART 5/7 OF THE ATT4S MATRIX IN EXCEL FORMAT.

Collection		Command and Control	
Adversary-in-the-Middle	Unauthenticated gateway or unauthenticated interplanetary node	TC/TM delay	
	Satellite constellation	Telecommand	GNC timeline
Data from link eavesdropping	Payload eavesdropping		OBCP modification
	Range Data eavesdropping		Update/patch channel
	TC/TM eavesdropping		

FIGURE 13 - PART 6/7 OF THE ATT4S MATRIX IN EXCEL FORMAT.

Exfiltration	Impact	
Exfiltration Over Payload Channel	Denial of Service	Direct Network Flood
Exfiltration Over TM Channel		RF Jamming
Side-channel exfiltration		Optical Jamming (Links/Sensor Blinding)
RF modification		Receiver flooding
Optical link modification		Receiver lock on a spurious carrier
		SDR buffer overflow
	Permanent loss to telecommand satellite	Replace session and master keys
	Resource damage	Breakdown of malicious/counterfeit hardware
		Receiver damage
		Space Debris Impact
		Physical sabotage
		Resource destruction
		Intentional collision with other satellites
	Resource Hijacking	Drain satellite's power
		Illegitimate bandwidth usage
		Waste of propellant
		Orbit Trajectory Manipulation
	Runtime Data Manipulation	
	Service Stop	Ground system loss
		Disabling Payload Service
	Temporary loss to telecommand satellite	Replace session keys
	Transmitted Data Manipulation	TC Data Manipulation
		TM Data Manipulation
		Range Data Manipulation
		Payload Data Manipulation

FIGURE 14 - PART 7/7 OF THE ATT4S MATRIX IN EXCEL FORMAT.

8 - THE ATT4S TOOLS

8.1 – THE WEBSITE

The matrix is built in an Excel format, which is useful for working and to quickly editing the Techniques; however, a more practical tool is used to easily display the matrix and interact with it.

MITRE has a functional website for the ATT&CK framework, published on a GitHub repository [32]. To facilitate our work, the software available on GitHub has been adapted in order to fit with the ATT4S matrix. The website is running, customized in graphic and functionality, on a server in ESA internal network, to have a local instance that can be helpful for analysis. The website is based on Pelican [33], a static site generator written in Python, that generates html pages keeping them ready to be showed when requested by HTTP.

The Pelican website is divided in modules, with a Python component for the processing part, and an html component to configure the page theme.

The original website has been built to show three matrices (Enterprise, Mobile, ICS), and to offer the possibility to choose the required platform (PRE, Windows, macOS, Linux, etc.). Currently this is not a requirement of ATT4S, and the local version of the website has been modified to show only the ATT4S version. The layout maintains the matrix structure previously shown, with the possibility of showing and hiding the various sub-Techniques. If any Technique/sub-Technique is clicked, another page opens, to display its detailed description of the objective and the threatened resource, in addition to links for references or standards.

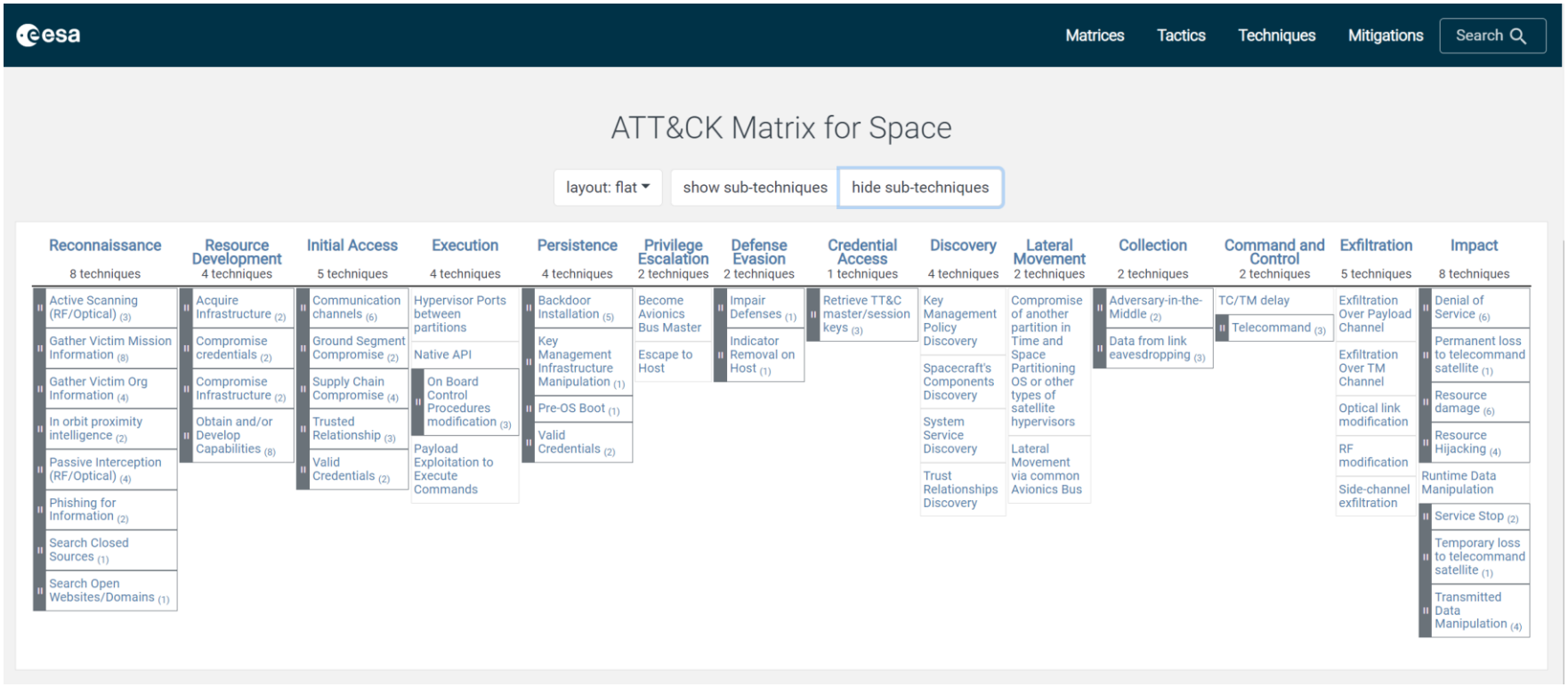

FIGURE 15 - THE ATT4S WEBSITE HOMEPAGE.

Every Technique is identified by an ID, that is the same of MITRE when the Technique is modeled from it, and a new one when the Technique is completely novel.

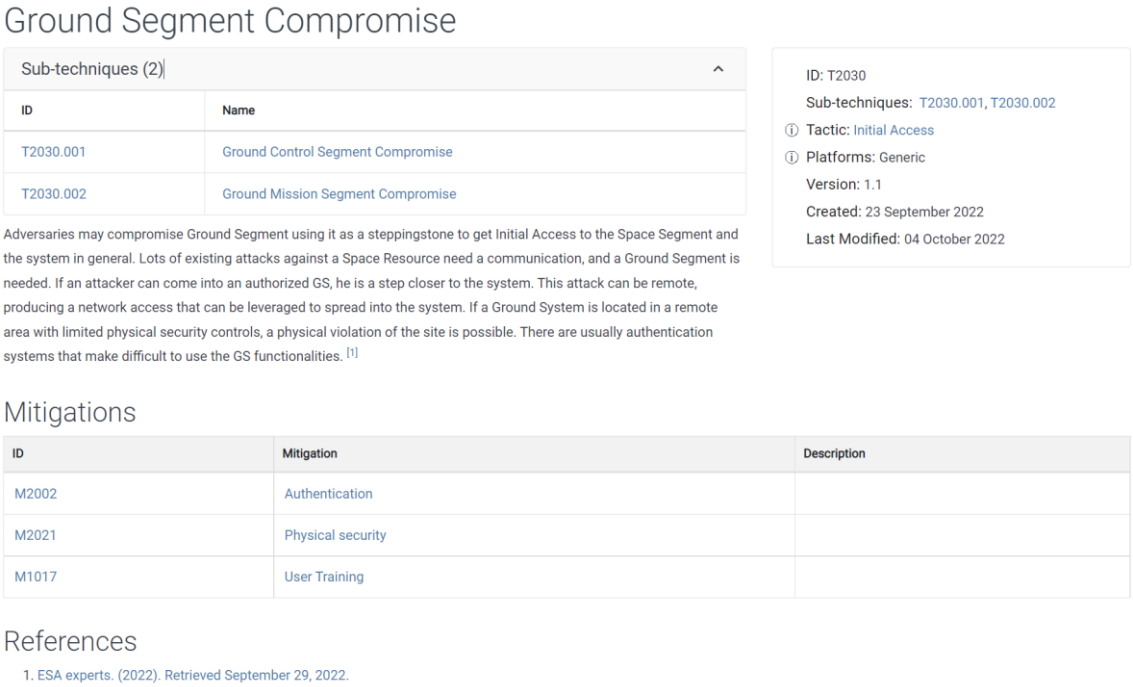

FIGURE 16 - EXAMPLE OF TECHNIQUES DISPLAYED BY THE ATT4S WEBSITE.

The Website is capable to show matrices in STIX [34], a standard language and serialization format used to exchange cyber threat intelligence. The matrix has been converted to STIX with another MITRE tool, the ATT&CK Workbench [35], that permits to insert the attack patterns and their relationships.

8.2 – THE WORKBENCH

The ATT&CK Workbench is a web graphical tool to extend the ATT&CK matrix. It helps to create, edit, and share Matrices, Tactics, Techniques, Mitigations, and relationships, exporting them as STIX files.

A Docker container is provided from MITRE, and a local instance is used to create from scratch the STIX version of the ATT4S matrix. The first step is to create a matrix, to collect all the components related to the space environment. Then, Tactics can be created, and inserted into the matrix. The following step is the Techniques creation, subsequently they are assigned to the related Tactic (only one or more than one). Mitigations can be written in the same way and connected with the relative Technique.

When the matrix is completed, it can be packed into a Collection, and all the previous components can be inserted or excluded from it.

The Collection is an exportable entity, resulting in a STIX formatted JSON file. The final file can be used as input for the Website and for the Navigator, or it can be imported again in a different instance of Workbench for an additional modification.

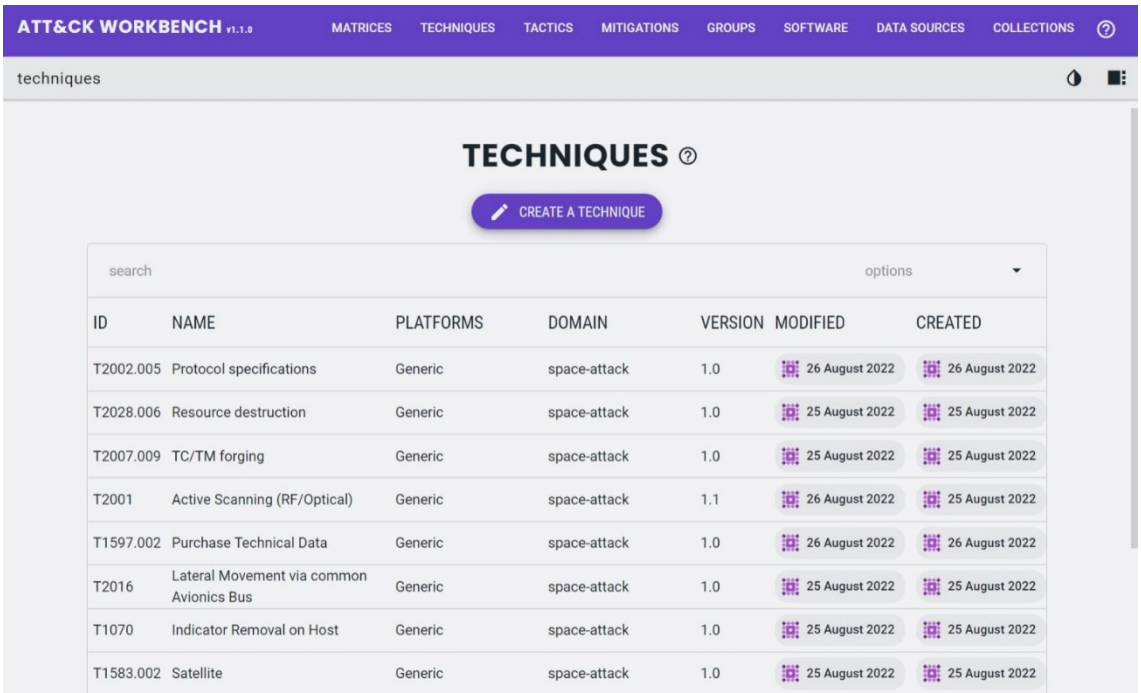

FIGURE 17 - ATT&CK WORKBENCH.

8.3 - THE NAVIGATOR

The ATT4S matrix is a structured knowledge of Techniques and can be used with the Website to search, navigate, and evaluate them.
A further tool is provided by MITRE, designed to navigate, annotate, and manipulate the matrix, the Navigator [36]. Scores and colors can be assigned to every Technique, to represent its likelihood, risk, or other indicators useful for a risk assessment.

A local instance of the Navigator has been launched on a server in the ESA network, leveraging the official Docker container. This instance permits to use the ATT4S matrix as a risk assessment tool.

FIGURE 18 - ATT4S MATRIX ON THE NAVIGATOR.

8.4 - ATT4S APPLICATION EXAMPLE

An example of possible use of the ATT4S matrix is the attack chain representation of a real jamming attack against communication satellites in Iran repeatedly over the years [37], the last time on an Eutelsat TV satellite on September 26th, 2022 [38]. When the jamming is orbital, it involves the transmission of a rogue signal towards the satellite uplink antenna to overpower the original source in the receiver. This kind of attack needs the knowledge of the satellite position and the frequency it uses to receive the TV signal. The RF communication channel is jammed, and the broadcasted signal is disrupted in the entire region of coverage.

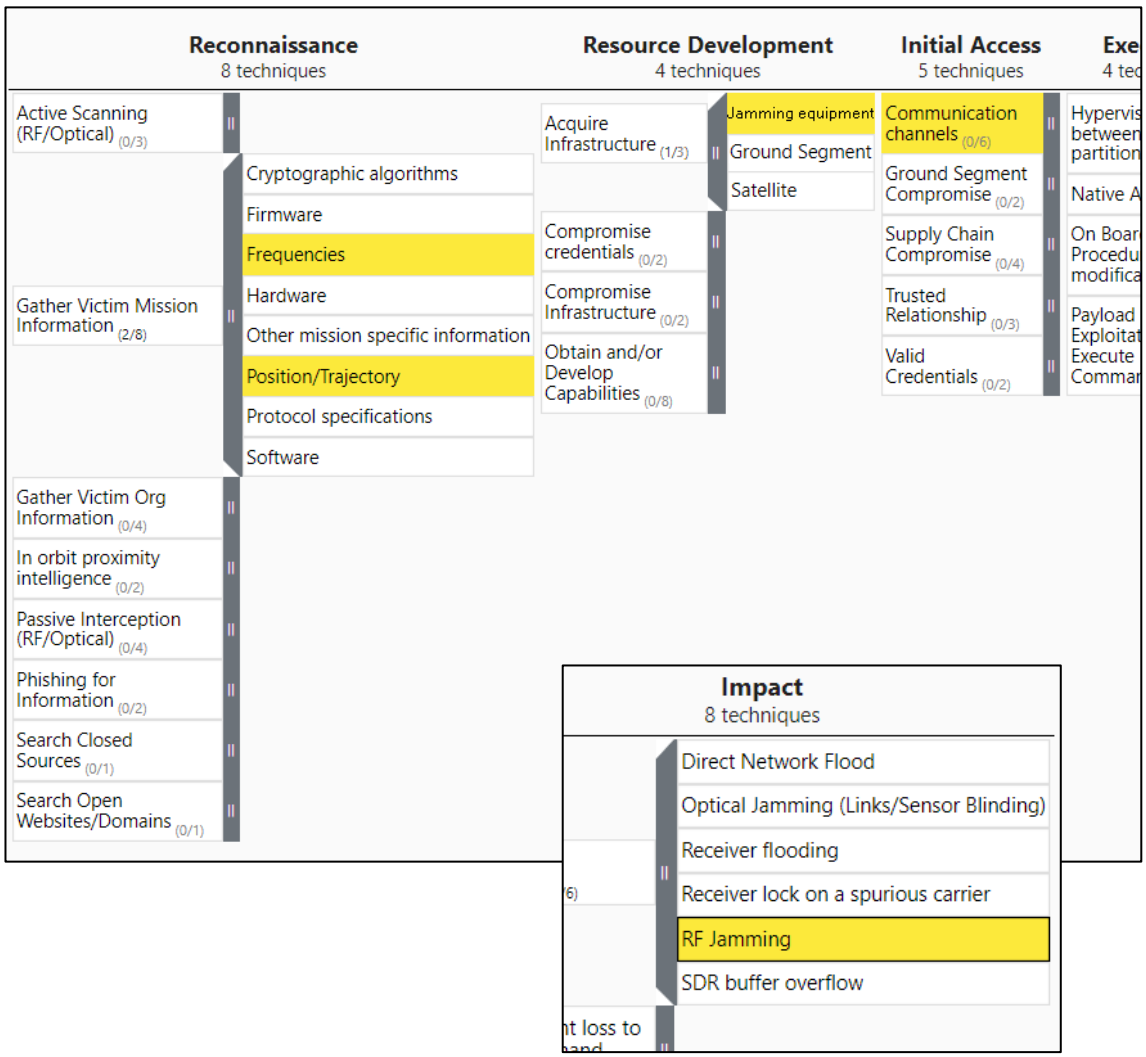

FIGURE 19 - JAMMING ATTACK ON ATT4S NAVIGATOR.

9 – CONCLUSIONS AND FUTURE WORK

9.1 - CONCLUSIONS

The objective of this project was the realization of a matrix to model Tactics and Techniques for the Space Domain, based on the ATT&CK framework.

A first version of that matrix, called ATT4S, has been produced, either as an Excel file and as a STIX-formatted JSON file. The matrix contains Techniques suitable for space systems, and each of them belongs to one or more Tactics. Every Technique is provided with a description, to offer more information and context, references to sources and to related CCSDS standards.

A first draft of the Mitigations has been included into the matrix, but further studies are needed. ATT4S is also published in an ESA LAN internal website, making it available for consultation and improvements. A local version of ATT&CK Navigator is also available and loaded with the last version of the matrix.

9.2 - FUTURE WORK

Further work could be done, to increase the detail of the information available in the matrix and to maintain it updated. The collection of Mitigations is in an initial phase, and it requires more research.

The ATT4S matrix is currently hosted in a generic virtual server, and it could be hosted on a “production” website, also provided with a fixed DNS to became easily reachable by users and in a more stable manner.

The matrix could be populated with further research on the applicable Techniques and should be constantly updated with new emerging Threats. ATT4S could also be detailed and branched to be more mission-specific or resource-specific. Other components can be considered and integrated, to make it broader. Considering the ATT&CK matrix, the following objects can be inserted: Procedures, Data sources, Groups, Software, Detections.

ESA is currently working on ATT4S, to produce a publicly releasable version.

REFERENCES

[1] THE MITRE CORPORATION, MITRE ATT&CK®, https://*attack.mitre.org*

[2] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *NIST Special Publication 800-39, Managing Information Security Risk*, March 2011

[3] BAILEY, B., J. SPEELMAN, R., C. COHEN, N., A. WHEELER, W., & A. DOSHI, P., *Defending Spacecraft in the Cyber Domain*, November 2019, Center for Space Policy and Strategy.

[4] MANULIS, M., BRIDGES, C., HARRISON, R., & AL., *Cyber security in New Space*, May 2021, Int. J. Inf. Secur.

[5] PALO ALTO NETWORKS, Cyberpedia, *https://www.paloaltonetworks.com/cyberpedia/what-is-mitre-attack-framework*

[6] AEROSPACE CORPORATION, Space Attack Research & Tactic Analysis (SPARTA), *https://sparta.aerospace.org*

[7] ENCYCLOPÆDIA BRITANNICA INC., *https://www.britannica.com*

[8] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *NIST Special Publication 800-30 Rev.1, Guide for Conducting Risk Assessments,* September 2012

[9] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, *ISO/IEC PDTR 13335-1:2004,* 2004

[10] WILFRIED LEY, KLAUS WITTMANN, WILLI HALLMANN*, Handbook of Space Technology,* 2009, John Wiley & Sons, Ltd

[11] SPACE EXPLORATION TECHNOLOGIES CORPORATION (SPACEX), *https://www.spacex.com*

[12] THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS), *SECURITY THREATS AGAINST SPACE MISSIONS, CCSDS 350.1-G-3,* 2022

[13] WIKIMEDIA FOUNDATION, INC., Wikipedia, *https://en.wikipedia.org*

[14] THE MITRE CORPORATION, Enterprise matrix, *https://attack.mitre.org/matrices/enterprise/*

[15] THE MITRE CORPORATION, *MITRE ATT&CK®: Design and Philosophy*, March 2020

[16] VMWARE, INC., *https://wwwvmware.com/topics/glossary/content/mitre-attack.html*

[17] THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS), https://*public.ccsds.org*

[18] EUROPEAN COOPERATION FOR SPACE STANDARDIZATION (ECSS), *https://ecss.nl*

[19] ESA Experts, interview with Thanassis Tsiodras, On-Board Computer & Data Handling Eng., TEC-SWT, 2022 May 23rd, ESA ESTEC

[20] ESA Experts, interview with Antonios Tavoularis, Real-time Embedded Software Eng., TEC-EDD, 2022 June 8th, ESA ESTEC

[21] ESA Experts, interview with Giacomo Da Broi, Security Systems Eng., TEC-ESS, 2022 July 1st, ESA ESTEC

[22] ESA Experts, interview with Juan Carranza, Software Eng., TEC-SWT, 2022 Jul 7th, ESA ESTEC

[23] ESA Experts, interview with Ignacio Aguilar Sanchez, Communication Systems Eng., TEC-ESS, 2022 May 13th and Jul 7th, ESA ESTEC

[24] THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS), *SPACE DATA LINK SECURITY PROTOCOL, CCSDS 355.0-B-2,* 2022

[25] AMAZON WEB SERVICES, INC., AWS Ground Station, *https://aws.amazon.com/ground-station*

[26] THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS), *CCSDS AUTHENTICATION CREDENTIALS*, *CCSDS 357.0-B-1,* 2019

[27] THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS), *CCSDS REPORT CONCERNING SPACE MISSIONS KEY MANAGEMENT CONCEPT, CCSDS 350.6-G-1,* 2011

[28] SECURITYSCORECARD, *https://securityscorecard.com/blog/6-strategies-for-cybersecurity-risk-mitigation*

[29] NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *Federal Inf. Process. Stds. (NIST FIPS) - 197,* 2001

[30] THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS), *CCSDS REPORT CONCERNING CRYPTOGRAPHIC ALGORITHMS, CCSDS 350.9-G-1,* 2014

[31] THE CONSULTATIVE COMMITTEE FOR SPACE DATA SYSTEMS (CCSDS), *CCSDS RECOMMENDED STANDARD FOR CRYPTOGRAPHIC ALGORITHMS, CCSDS 352.0-B-2,* 2019

[32] THE MITRE CORPORATION, ATT&CK Website, *https://github.com/mitre-attack/attack-website*

[33] JUSTIN MAYER, Pelican, *https://getpelican.com*

[34] THE MITRE CORPORATION, Structured Threat Information Expression (STIX), *https://stixproject.github.io*

[35] THE MITRE CORPORATION, ATT&CK Workbench, *https://github.com/center-for-threat-informed-defense/attack-workbench-frontend*

[36] THE MITRE CORPORATION, ATT&CK Navigator, *https://github.com/mitre-attack/attack-navigator*

[37] *https://smallmedia.org.uk/sites/default/files/Satellite%20Jamming.pdf*

[38] *https://www.eutelsat.com/en/news/press.html#/pressreleases/please-find-below-a-statement-from-eutelsat-3209454*