Ground Station as a Service Reference Architectures and Cyber Security Attack Tree Analysis

Nicolò Boschetti
Johns Hopkins University
Baltimore, MD, USA
nbosche1@jhu.edu

Chelsea Smethurst
Microsoft
chelsea.smethurst@microsoft.com

Gregory Epiphaniou
University of Warwick,
Coventry CV4 7AL, U.K
gregory.epiphaniou@warwick.ac.uk

Carsten Maple
University of Warwick,
Coventry CV4 7AL, U.K
CM@warwick.ac.uk

Johan Sigholm
Dept. of Systems Science for Defence and Security
Swedish Defence University
Stockholm, Sweden
johan.sigholm@fhs.se

Gregory Falco
Johns Hopkins University
Baltimore, MD, USA
falco@jhu.edu

***Abstract*—As the Ground Station as a Service (GSaaS) paradigm transforms space infrastructure operations, new attack surface emerges for malicious actors. While the space community generally refers to GSaaS as a singular model, there are several flavors of these systems. After a description of the general GSaaS network's basic structure, this paper presents an analysis of four reference architectures of GSaaS. On the basis of this systems engineering analysis, a cybersecurity analysis of the critical nodes will be carried out through the attack tree method. Later the cybersecurity implication both of technical and strategic characteristic of GSaaS networks will be discussed and put in relation with the current state of space cyberwarfare landscape.**

TABLE OF CONTENTS

1. INTRODUCTION

This study identifies the risks associated with the multiplication of commercial satellite ground stations all around the globe. Ground stations are a fundamental component of space operations, and with the current growth of satellites, especially in Low Earth Orbit (LEO), more and more operators require systems to downlink their data to Earth. This has led to the emergence of private ground station networks that offer the so-called Ground Station as a Service (GSaaS) that flanks the existing government-owned infrastructures. To contain the massive costs, satellite operators that lack communication ground segments buy slots in GSaaS antennas for communications and downlink operations with their satellites. These services are offered by private operators equipped with a proprietary network or aggregating a large number of third-party satellite ground stations into a single network, simultaneously ensuring global coverage and low costs. This research analyzes the cybersecurity profiles of different GSaaS architectures utilizing an attack tree approach.

In this work, first, we build an architectural model of different types of satellite GSaaS networks. Subsequently, this division allows us to detect particular attack vectors for each typology in the cyber domain. GSaaS is becoming increasingly vital for defense actors in many domains of operation such as Earth observation and electronic intelligence data relay. Therefore, the dual-use nature of these activities and infrastructures, in addition to generating an additional layer of risks, makes an analysis of the current security profile of this sector of the space economy even more urgent. Hence, this research will also discuss the implications that the growing dual-use nature and significance for critical infrastructure functions have on GSaaS services. The growing importance of satellite services for economic, military, and critical activities means that any attack on satellite ground stations will also have severe repercussions on sectors of society and markets outside the space sector.

2. METHOD

We combine data from various open-source business and commercial resources with academic research and open-source intelligence sources. The outcome, obtained through a systems engineering approach, consists of an architecture analysis of the GSaaS sector. After linking this analysis with risk categories and documented hostile practices, we present an attack tree analysis for a specific case-study that refers to the architectures' essential components. Security knowledge basis such as MITRE ATT&CK[1] and Aerospace Corporation's SPARTA[2] have been particularly useful in informing the attack tree analysis.

3. BACKGROUND

The basic architecture of a space mission has remained unchanged since the time of the first Sputnik in 1957. A spacecraft launched into space has to communicate with the ground through electromagnetic waves. This constitutes the three primary segments of space activities: Space (the spacecraft), Link (the signal), and Ground (the antenna and the mission control)[3].

978-1-6654-9032-0/23/$31.00 ©2023 IEEE

During the decades, thanks to the progressive commercialization of space activities, the cost of designing, assembling, and launching a satellite has become lower. The only segment that, still today, remains significantly complex and consequently expensive is the ground one, especially in its Telemetry, Tracking & Control sub-component. The solution generated by the market was that of Ground Station as a Service; a distribution and commercialization of satellite communications[4]. If, in the past, a space operator had to install and manage its own ground segment, now, thanks also to the increase of satellites in orbit, Satellite ground stations have become a separate sector of the space economy. Commercial entities equipped with terrestrial satellite networks, often with global coverage, offer satellite operators to use their infrastructure for downlinking and uplinking data. This commercialization of satellite communications is not a recent phenomenon, but its technical evolution in the form of virtualization is. Now not only communications with satellites are outsourced to third-party providers, but thanks to the virtualization of ground stations, mission control can also be managed through non-proprietary infrastructure[4]. For example, the emergence of cloud technologies, increased performances and speed of broadband networks, and other technological advances have ensured that through the internet, an operator in Australia can control its satellites through a link through a ground station in Iceland[5].

The market is currently divided between numerous companies of different sizes, nationalities, offers, and above all, architectures. Each company has proprietary protocols and a slightly different sub-component organization. In this study, we proceeded to generalize the possible architectures into four categories:

1. Single GS Provider Semi-Virtualized (**Figure 1**)
2. Single GS Provider Fully Virtualized (**Figure 2**)
3. Multi-GS-Provider Fully Virtualized (**Figure 3**)
4. Heterogeneous Open-Source Semi-Virtualized (**Figure 4**)

In the first category, we can mention, for example, the Swedish Space Corporation (SSC) network that offers partial virtualization of the ground station network through third-party cloud services but simultaneously allows a legacy interaction with the end user and separate management of mission operations[6]. In the second category, companies such as Kongsberg Satellite Services (KSAT)[7] and Leaf Space[8] own a ground stations network and offer virtualized services with proprietary cloud systems. The multi-provider fully virtualized category is very similar to the second, with the difference in aggregating the capacity of different GS networks in a single commercial cloud-based architecture. In this category, the most prominent actors are Microsoft Azure[9] and Amazon Web Services (AWS)[8]. Finally, the fourth category is still not commercialized but mainly amateurish and scientific research oriented. The most important example is the ESA-awarded SatNOGS network, which is open-source, collaborative and COTS-based[10].

4. Ground Station as a Service Basic Segments and Components

A GSaaS network is an example of a System of Systems. Each segment of a space mission needs to be coordinated with others, and this integration is necessary at the level of subsystems, components, and human operators. Space, Link, Ground, and User segments are all involved in the operations of GSaaS, leading to the overlapping some traditional barriers between segments. In fact, the great novelty of this space activity is the virtualization of many operation phases that leads to sharing responsibilities among different actors.

Since the beginning of space activities, dozens of common or exclusive risk categories have been identified for all segments of a space mission[11]. They may be related to the physical integrity of the infrastructure or its operation and may, for example, be of an environmental or cyber nature. A GSaaS architecture does not augment the number of these risk factors but coagulates them in one single SoS[5]. This makes the risk factors interconnected, increasing their cascade effects on the various segments and components. Therefore, the GSaaS risk area is greater than the risk area of all components taken individually. Systems interconnection makes the whole greater than the sum of its parts. However, as we shall see, this can also increase the redundancy and the number of security and prevention measures put in place to protect the system.

Before describing the different possible architectures and, subsequently, the peculiarities of their security, we will briefly define the different segments. Traditionally a space infrastructure is divided into three primary segments: space, link, and ground plus, but not always, the user. However, by addressing GSaaS architectures and performing security analysis, we found that this distinction needs to be updated. In a virtualized GSaaS architecture, the ground segments' TT&C and data handling and processing components have substantially different architectures. The virtualization even generates an overlapping of user and ground segments. Because of this, we broke down a GSaaS architecture into five fundamental segments

- Space Segment: the satellite or the constellation;
- Link Segment;
- Telemetry, Tracking, and Control (TT&C) Segment: the data acquisition and sending;
- Data Handling and Storage Segment (DH&SS);
- End User Segment.

Space Segment

The growth in the number of satellites and the increasing presence of satellite constellations, sometimes composed of hundreds of spacecrafts, makes the space segment particularly complex. This complexity is both technical and related to the safety of operations. Whether the satellite is in LEO, MEO, or GEO, it constantly depends on other vehicles in orbit. This connection may be necessary for orientation purposes such as positioning, navigation, and timing (PNT) or to share information within a constellation through radio crosslinks[3]. However, the interaction with other objects can also be a risk to the safety of operations. In addition to the ever-increasing hazard posed by orbital debris, a satellite can also be the victim of hostile Rendezvous and Proximity Operations (RPOs) by an attacker[11]. This growing interaction between different systems in orbit and the increased number of threats to their integrity and operability also has consequences on all the other segments that constitute the mission architecture.

Link Segment

It is constituted by the data flow between the satellite and the ground stations. This data exchange between the two nodes is bi-directional and can be achieved through different means. The most used technology is Radio Frequency (RF) modulation, and microwave and optical links are also being

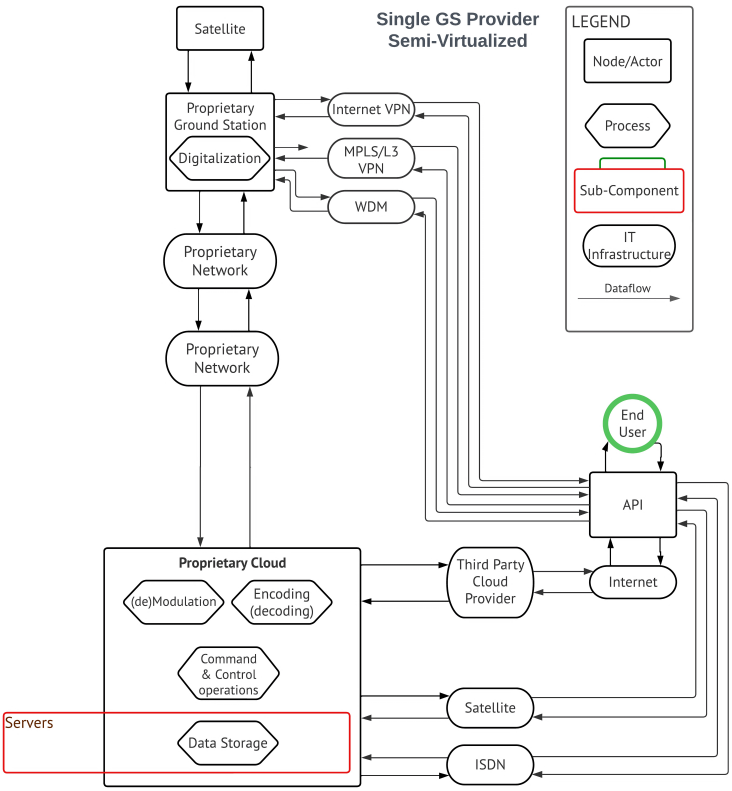

Figure 1: **Single GS Provider Semi-Virtualized Architecture**

developed and deployed[3].

A GSaaS does not present novelties in this segment compared to other architectures, but the operating RF bands are usually a crucial component of the commercial offer. For example, Ku and Ka-bands are commonly preferred for data-heavy downlink requirements, while UHF and VHF communications are sufficient for telemetry acquisition and RF tracking.

Telemetry, Tracking, and Control (TT&C) Segment

This segment is constituted by the Ground Stations physical components such as the antenna, the amplifiers and the modems. Its design and composition, even if generalizable, varies depending on the choices of the single network provider. For example, ground stations can be equipped with edge components that allow actions usually carried out by the Data Handling and Storage Segment in a virtualized and semi-virtualized architecture. This can lead to hybrid solutions that add redundancy to some operation phases but also multiply the network's attack surface.

This segment's essential functions consist of being one of the Link segment's endpoints, collecting RF data, digitalizing them, and being connected to the network to communicate with the DH&SS segment.

Data Handling and Storage Segment

This segment is the core of a GSaaS architecture. Connected to the TT&C and User segments, it collects, stores, handles, and shares the satellite data. It also collects and generates the uplink data, commands, and updates, carrying out mission control functions. Both in semi-virtualized and a virtualized architectures its basic components are the data center and the eventual cloud computing and storage services. In a virtualized architecture all the Data Processing, Analytics and Storage functions are hosted in the cloud. It can also host Mission and Command & Control Operations that are then relayed to the satellite through the TT&C and Link segments. Another fundamental function of this segment is the Data Sharing that makes possible the interaction with the User Segment through different means of connection.

User Segment

This segment refers to the end users of the network. It comprises the users' equipment, the software, the API and the network endpoints that interact with the DH&SS segment. In a virtualized GSaaS network it sometimes overlaps the third segment since, through cloud-based software and tools the end user is able to directly interact with data or perform mission control operations.

5. Reference Architectures

In our study, we identified four key types of GSaaS architecture that are currently operational. They differ in the homogeneity of the ground control operators, the degree of virtualization, and the organization of the network.

Single GS Provider Non-Fully Virtualized GSaaS

This type of architecture, shown in **Figure 1** has been on the market for more time and has the highest degree of separation among its components.

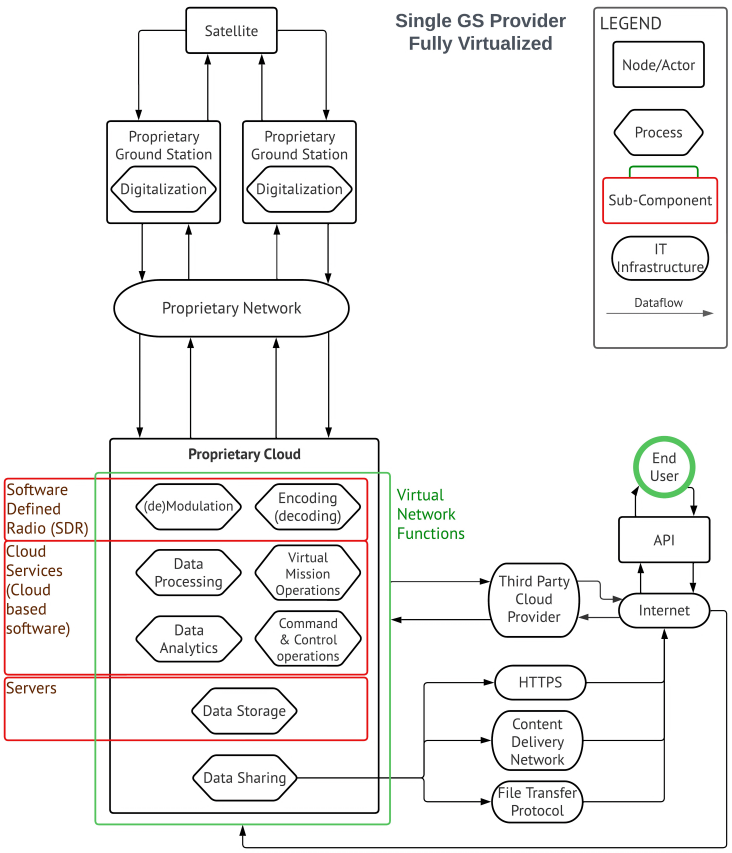

Figure 2: **Single GS Provider Fully Virtualized Architecture**

A satellite communicates with a network of ground stations owned by the GSaaS provider. Usually, the ground stations, distributed around the globe to make it possible that the satellite is almost constantly in sight of a GS, are equipped with edge components. Each ground station is consequently provided with the means to carry out autonomously digitalization, modulation, encryption, and basic handling functions on data. Even if it can spread the possible attack surface, this enables these extreme architecture nodes to communicate directly with the end users bypassing the data center.

The TT&C segment is connected with other segments in two ways. First, it can directly relay information and data to the end users through different communication systems such as fiber optic or internet VPNs. Second, it can relay the information to the data center and the Mission Operation Control (MOC) through a proprietary ground backbone or internet. Usually, the ground stations of the same network are interconnected to the internet by Points of Presence (PoP) that act as collectors of data streams. This, beyond coordination and cost reasons, is necessary due to the often remote position of the ground stations.

If not directly relayed to the end user, the downlinked data are transferred from the PoPs to the data center. In the case it has not happened before, here data are demodulated, decoded, stored, and shared. In this architecture, this segment is also responsible for Mission Control and Command and Control Operations without the direct intervention of the users that we will describe in the following architecture.

There are several options for Data Sharing with the User segment. End users can access their data stored in the servers through protocols such as File Transfer Protocol (FTP), Content Delivery Network (CDN), HTTPS, Satellite Relay (VSAT), Integrated Services Digital Network (ISDN), Multiprotocol Label Switching (MPLS), or third-party cloud services such as Microsoft Azure or Google Cloud. Apart from satellite relays, the customer accesses the data using the preferred protocol through the internet network and often an API provided by the operator.

This is the architecture with the lowest level of interaction between the user and the other segments. Data can be accessed, requested, and even sent, but without direct manipulation or active participation in the mission operations.

Single GS Provider Fully Virtualized GSaaS

This architecture, shown in **Figure 2**, represents an evolution of the previous one made possible by the emergence of cloud computing technologies and advancements in network capabilities.

The space, link, and TT&C are not substantially different from a semi-virtualized architecture, except that edge components in the ground stations are rarely used and often adopted to augment the system's redundancy. Ground stations are organized in global or regional networks. More frequently, in regional or area-subdivided networks, the connection to the DD&SS segment is made possible by ground proprietary links to achieve higher data transfer speed and reliability.

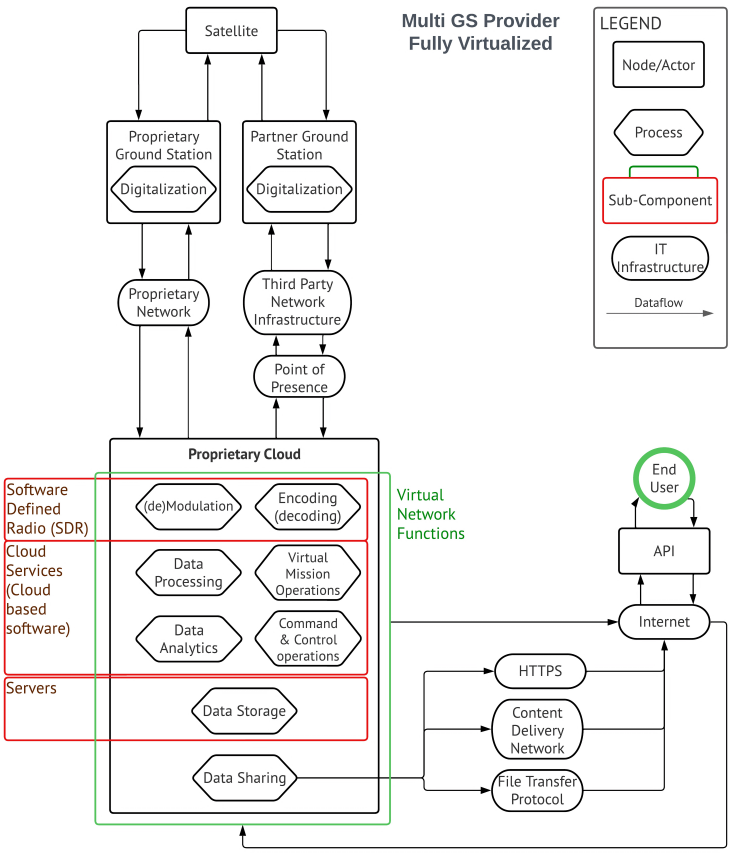

Figure 3: **Multi GS Provider Fully Virtualized Architecture**

After the transfer of downlinked data to the data center, they are demodulated, decoded, decrypted, and stored. Even if traditional systems of data sharing, such as FTP or CDN, persist, the main characteristic is the virtualization of ground station functions. The end user, in fact, can get access to the data through a cloud-based infrastructure that allows directly handling and analyzing data. This overlapping of user and DD&SS segments consents the first to perform mission operations or manage the C2 procedures directly. This is made possible by the presence of cloud-based software, Artificial Intelligence and Machine Learning functions and other data and mission operations tools.

The user can access and operate in the cloud through the internet using different protocols and VPN tools similar to the previous architecture. In addition, the operator usually provides APIs and GUIs that facilitate the interaction with the different functions. In some cases, the provider's cloud can be integrated with third-party cloud services that host the API, the GUI, and the data-sharing functions.

This architecture, together with the following, presents the highest interaction level between the different GSaSS network segments. The most diverse and complete are the virtualized functions, the most similar the user experience is to a classic, fully integrated, and owned space mission architecture.

Multi GS Provider Fully Virtualized GSaaS Network

This architecture, shown in **Figure 3**, is organized substantially in the same way as the previous one, with a considerable difference: the integration of ground stations of different providers.

Through the aggregation of different satellite ground networks, or sometimes even isolated antennas, a GSaaS provider can augment its coverage and total radio bandwidth. More coverage and bandwidth make possible a more significant number of satellite links and consequently higher amounts of data but pose technical and security issues. The first problem to overcome is the coordination between different ground architectures. For example, distinct GS providers may have different data management and encryption protocols that can hinder interoperability. In the same way, security practices and procedures can be an obstacle for attackers as for partners. The second problem is related to the security of the data flow, as will be illustrated in greater detail later; in such architecture, the GSaaS provider loses the ability to control the security of the handled data fully. Again, this generates risks both for the provider and the end users.

Similarly to the previous architecture, the GSaaS provider provides a cloud-based data handling and sharing platform that a proprietary data center hosts. The data center here serves not only as a hub for data but also as a crucial coordination node for sharing requests, information, and parameters between different architecture nodes. This coordination is even more critical if, among the offered cloud-based services,

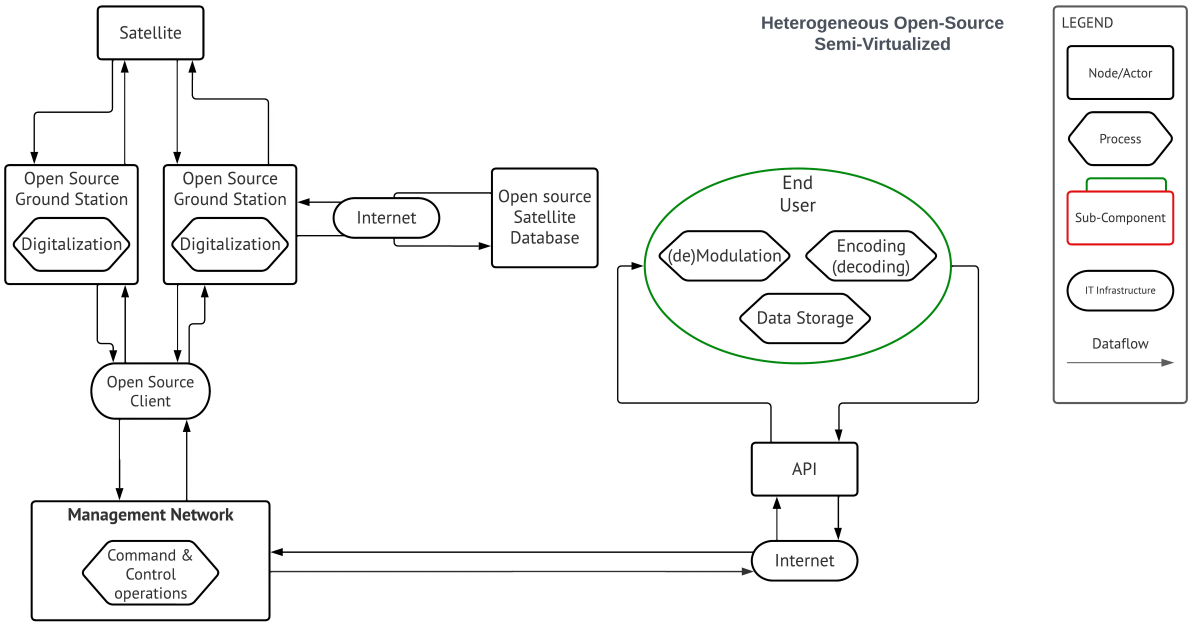

Figure 4: **Heterogeneous Open-Source Semi-Virtualized Architecture**

there are Virtual Mission Operations (VOC) since satellite commands and updates could have to be uplinked through third-party ground stations.

Heterogeneous Open-Source Semi-Virtualized GSaaS Network

Although this architecture, shown in **Figure 4**, has not yet become of commercial interest, it is still of technical and security interest. By "Heterogeneous," we mean a widely fragmented and assorted control of the ground stations. "Open-Source" is what makes this diversified control possible, allowing the construction and dissemination of cheap and simple systems to private users. Finally, the "Semi-Virtualization" is given by the necessary internet-based coordination of ground station communication and observation functions and the absence of cloud-based DD&CC segments.

The already cited SatNOGS network is the most prominent example of such architecture. In this collaborative and no-profit network, GS providers and users frequently overlap. Operating in UHF and VHF bands, this network aims at amateurish data downlinks from CubeSats or scientific LEO satellites.

The ground station is elementary and composed of an antenna, a rotator, a Raspberry PI or PC, and a software-defined radio. In addition, the community provides the users with a specific client to access the network[12]. The owner of the ground station is often the user attempting a connection with the desired satellite: consequently, link, TT&C, and user segments overlay. In this architecture, the DH&SS segment mainly consists of a Management Network that controls the observation operations of the ground stations. In addition, the ground station is aided in its functions by access to open-source databases of RF bands and orbits: a surrogate of Space Situational Awareness and Tracking functions. All network nodes are connected by public internet access via an open-source client.

6. GSaaS Cyber Attack Tree Analysis

Attack Tree Method

Attack tree analysis consists of an approach useful to enumerate various attack pathways for an attacker to achieve a goal[13]. The attack goal is stipulated at the top of the tree, while sub-goals are enumerated beneath, which are called branches. Each branch contains a series of leaf nodes, representing actions required to achieve the sub-goals. Leaf nodes that must be performed together to accomplish a sub-goal are joined by an "AND" gate, whereas leaf nodes representing distinct choices are represented by an "OR" gate.

Attack trees are a derivation of fault tree analysis, a common approach in the aerospace community to identify flaws in complex systems. Fault trees were developed in 1962 at Bell Telephone Laboratories while devising a method to determine failure modes and risks for intercontinental ballistic missiles (ICBMs)[14]. They have previously been used to analyze the security profile of space systems[15].

The main weakness of this method is the risk of resulting static and highly subjective[16]. To reduce the subjectivity of attack trees, researchers have standardized their components, which facilitates comparison across different systems and their scalability across many systems, as we did in this research. Furthermore, the proposed attack methodology uses existing security frameworks, matrices, and taxonomies to enable consistency and ground-proved risks.

Given the different system architectures, we selected a case study of an attack goal relevant to a Ground Station as a Service network. Usually, attack trees focus on a system or a single subsystem; in this case, we decided to connect different attack trees related to the same attack goal. This completes the Defense in Depth analysis that shows how an SoS like a GSaaS architecture presents at the same time a multitude of attack vectors but also of protection layers.

	(1)	(2)	(3)	(4)
a) Satellite	No	No	No	No
b) Ground Station	Yes	Yes	Shared	Shared
c) Ground Backbone	Yes	Yes	Shared	Public
d) Point of Presence	Yes	Yes	Shared	X
e) Data Center	Yes	Yes	Yes	Yes
f) Cloud	No	Yes	Yes	X

Table 1: Provider Control over Architecture Nodes

The attack trees are described in sequence, following the data flow from the satellite to the end user. Some of the sub-goals achieved by the attacker after completing one subsystem or segment tree can be used to complete a subsequent attack goal on a different part of the architecture. The attack trees described are not a fully comprehensive depiction of the entirety of attack vectors and techniques but prove the interconnection of the different GSaaS components.

Case Study: False Data Injection

Given the four system architectures described in section IV, we selected a representative attack scenario: false data injection.

We generalized the first three architectures by identifying the six nodes shared by each one and fully or partially controlled by the GSaaS provider. Partially controlled nodes can be the ground station and the cloud. We assume, in this case study, that even if the control is partial, the security practices adopted by the third-parties are shared with the GSaaS provider and efficiently carried out. Even if the satellite is usually not owned or fully controlled by the GSaaS provider, it is an essential component of both the space and link segment. It is assumed that the only endpoint of the link segment is constituted by the company's ground stations, giving the provider higher security and protection privileges.

The nodes analyzed in the attack tree are:

1. Satellite and Link Segment
2. Ground Station
3. Ground Backbone
4. Point of Presence (PoP)
5. Data Center
6. Cloud

The chosen attacker's goal is a False Data Injection (FDIA). It consists in compromising the data collected, transmitted, or generated by a system. An FDIA can be aimed at many systems, such as power or industrial control systems[17], but its consequences are highly variegated in a space system. For example, it can alter the data acquired by an EO mission, insert false data in an ML algorithm hosted by a GSaaS cloud platform, or deceit a Space Situational Awareness system[18]. The same attack on different segments and nodes can have different outcomes.

The attack tree for a false data injection is shown in **Figure 5** and **Figure 6** in the **Appendix Section** and depicts the actions that an attacker would perform in order to achieve their goal. Each sub-tree describes the actions needed in a specific node. The goal is the same for each node.

The attack tree presented in this study focuses on the cyber component of the system's security. With the aim of focusing the attention to the nuances that characterize GSaaS architectures in comparison with other satellite ground station networks, we have overlooked physical threats like the kinetic destruction of the antennae or disruption of energy supply. Every technique listed in this analysis is cyber or strictly aimed at providing the attacker with better capabilities for following stages of the hostile action.

The attack is composed, for each segment, of four main actions:

- Reconnaissance
- Deliver
- Exploit
- Execute

In the detail:

- **Reconnaissance** consists of learning about the architecture assets and collecting access credentials. Then, the attacker is equipped to deliver the attack through techniques such as cyber social engineering or the insertion in the supply chain.
- **Deliver** consists of delivering the attack method to the system. To achieve the goal of injecting false data, the methods are multiple. The techniques for delivering the attack change depending on the subcomponent and the type of false data that needs to be delivered. Once delivered the weapon to the targeted node, the attacker is ready to exploit it.
- **Exploit** consists of penetrating the system and, consequently, the many protective layers previously described. The techniques adopted heavily depend on the targeted node's nature. For example, in the satellite/link segment, exploitation through the installation of malicious software will be challenging, while it is one of the primary attack vectors in the cloud segment. Once inside the system, the attacker is ready to achieve the goal.
- **Execute** consists of carrying out the last necessary actions to achieve the attack's goal. As for "exploit," the techniques are heavily influenced by the system under attack. Again in the cloud example, the execution can be performed in two very different ways. The attacker can decide to deliver the corrupted data directly in the data storage and access function of the cloud interface or, more subtly, run a software to act on data processing functions.

GSaaS Security Considerations

The attack tree described in the previous section is not architecture-specific but refers to six elements common to all commercial GSaaS architectures. However, this poses the problem of establishing a criterion to assess the differences in security between the different architectures. Leaving aside differences in the specific protocols and practices adopted by individual companies, it is possible to use a variable that is also generalizable: the direct control of the sub-components.

As shown in the **Table 1**, in different architectures, providers have different control over the individual nodes of the system. For example, a multi-provider architecture unites the services of different companies, at the same time, stratifies different security management practices. As a result, the GSaaS company, unable to control these practices, can rely only on contractual obligations with third-party providers. This partial control over the system's security can be extended to any architecture component, be it the TT&C segment or the cloud service used. The problem is exacerbated by the fact that, as already shown, a GSaaS network to be operational must be composed of antennas located on the entire planet. In the case of multi-provider services, this may mean that

there are actors from different nations with different standards of cyber and industrial security among third-party providers. The geographical fragmentation of these services, like in the Japanese company Infostellar, can hamper the success of the company's security practices and mitigation measures.

International organizations such as the International Telecommunication Union (ITU) or private consortia such as the Digital Intermediate Frequency Interoperability (DIFI) Consortium [19] work to unify practices, support the application of technical standards and foster interoperability. However, there is still considerable fragmentation in the cyber standards and practices applied to the space sector. Currently, in the absence of an international cybersecurity standard specific to space infrastructures, it can be difficult for a GSaaS company to assess the levels of security of a GS third-party provider.

As stated at the beginning of this research, the overall security of a System of Systems is not a simple aggregate of the single components securities. Consistency is needed between the different practices and layers described in the DiD analysis. One-stop management allows, for example, faster and more efficient management of Intrusion Detection Systems (IDS) and safer management of system updates or security patches. It can therefore be concluded that the less network fragmentation among different actors, the greater the theoretical security of the system.

7. GSaaS Risk in Context

As we previously said, the growth of satellites in orbit and the lowering of development and launch costs have led to the birth of the GSaaS sector. However, all this is accompanied by an increase in critical infrastructure reliability and multiple economic and military activities on space-based systems. For example, Earth Observation (EO) is increasingly an integral part of agricultural activities or climate sciences as, thanks to the increase in satellites, the same point of the planet can be monitored several times a day. This is of particular interest to military operations, as observation of enemy activities from space can provide crucial advantages in a conflict.

As for ground stations, there is increasingly widespread commercialization of these activities, both in the civil and military fields. Continuing the Earth Observation example, private companies such as Maxar or Planet provide EO services to the US National Recoinnassance Office (NRO) and other NATO armed forces[20]. Since these dozens of satellites in LEO have to communicate on the ground daily large amounts of data in the shortest time possible, they often use GSaaS networks[21]. The military nature of the received, processed, and stored data also makes GSaaS a dual-use space activity field. Hence, this dual nature dramatically increases the variety of possible attackers and their reasons. For this reason, the security of these infrastructures is increasingly critical. An attack like the one described in this study could have dramatic consequences for both civilian and military actors.

An example of false data injection into space assets is the attack on the Viasat Ka-Sat network a few hours before the Russian army invaded Ukraine in February 2022. Although it has not been directed against a GSaaS network, the techniques adopted to access the space and link segment to deliver malware at the end user terminals are ominously similar to those described above[22]. Exploiting vulnerabilities in control centers and points of presence allowed Russian hackers to reach the user segment and disable it. This action had heavy tactical consequences, disabling part of the C2 links of the Ukrainian army while having side effects on the energy infrastructure of other European nations. Therefore, the case study presented in this study has a historical precedent that demonstrates both the feasibility, the utility, and the fact that, in a war context, dual-use commercial infrastructures are considered full-fledged war targets, especially in the cyber domain.

8. Conclusion

The role of Ground Station as a Service networks for satellite communications and space activities, in general, is growing. This is coupled with the increasing reliance of many critical infrastructures and services on space assets. Hence, GSaaS is a likely target of space and cyber warfare. In this paper we have studied cyber security aspects of different satellite GSaaS networks. This was done by constructing architectural models for four key GSaaS architectures and analyzing their respective attack surfaces. In a subsequent case study, we performed an attack tree analysis of false data injection, an attack scenario representative for all the presented architectures.

Although establishing common assessment criteria for security analysis of different architectures is identified as a challenge, we conclude that a viable approach when performing a GSaaS security risk analysis is to address the generalizable variable of provider sub-component control. Providing detailed descriptions of different GSaaS architectures, including provider control over space and link segment components, is thus fundamental to inform a robust security risk analysis. The attack tree developed in this research is a first stab at the problem.

While the technical details are still uncertain, a so-called Hybrid Space Architecture (HSA) has been proposed by U.S. Department of Defence to reduce single points of failure across a satellite service ecosystem, and thus increase security and resilience of satellite communication and sensing services[23]. Future work includes outlining parameters of such a hybrid architecture and evaluating the potential gains in comparison to the GSaaS architectures presented in this paper. As future work we also propose a deeper analysis of the attack vectors of each different architecture, evaluating such aspects as the geographical dispersion of the TT&C segment, and the use of COTS components and software. The rising dual-use nature and the current international tensions make this fundamental for the security and resilience of the entire space community.

References

[1] The MITRE Corporation, "Att&ck." [Online]. Available: https://attack.mitre.org

[2] Aerospace Corporation, "Sparta." [Online]. Available: https://sparta.aerospace.com

[3] B. Elbert, *The satellite communication ground segment and earth station handbook*. Artech House, 2014.

[4] O. Kodheli, E. Lagunas, N. Maturo, S. K. Sharma, B. Shankar, J. F. M. Montoya, J. C. M. Duncan, D. Spano, S. Chatzinotas, S. Kisseleff, J. Querol, L. Lei, T. X. Vu, and G. Goussetis, "Satellite communications in the new space era: A survey and future challenges," *IEEE Communications Surveys Tutorials*, vol. 23, no. 1,

pp. 70–109, 2021.

[5] E. Meyrick, A. Pickard, T. Rahloff, S. Bonnart, A. Carlo, and K. Thangavel, "Ground station as a service: A space cybersecurity analysis," 10 2021.

[6] Swedish Space Corporation, "Website." [Online]. Available: https://sscspace.com

[7] Kongsberg Satellite Services, "Website." [Online]. Available: https://www.ksat.no

[8] Leaf Space, "Website." [Online]. Available: https://leaf.space

[9] Microsoft Azure Space, "Website." [Online]. Available: https://azure.microsoft.com/en-us/solutions/space/

[10] SatNOGS, "Website." [Online]. Available: https://satnogs.org

[11] G. Falco and N. Boschetti, "A security risk taxonomy for commercial space missions," in *ASCEND 2021*, 2021, p. 4241.

[12] D. White, C. Shields, P. Papadeas, A. Zisimatos, M. Surligas, M. Papamatthaiou, D. Papadeas, and E. Kosmas, "Overview of the satellite networked open ground stations (satnogs) project," 2018.

[13] T. R. Ingoldsby, "Attack tree-based threat risk analysis," *Amenaza Technologies Limited*, pp. 3–9, 2010.

[14] W.-S. Lee, D. L. Grosh, F. A. Tillman, and C. H. Lie, "Fault tree analysis, methods, and applications a review," *IEEE transactions on reliability*, vol. 34, no. 3, pp. 194–203, 1985.

[15] G. Falco, A. Viswanathan, and A. Santangelo, "Cubesat security attack tree analysis," in *2021 IEEE 8th International Conference on Space Mission Challenges for Information Technology (SMC-IT)*. IEEE, 2021, pp. 68–76.

[16] L. Piètre-Cambacédès and M. Bouissou, "Beyond attack trees: dynamic security modeling with boolean logic driven markov processes (bdmp)," in *2010 European Dependable Computing Conference*. IEEE, 2010, pp. 199–208.

[17] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, 2017.

[18] J. Pavur and I. Martinovic, "On detecting deception in space situational awareness," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 2021, pp. 280–291.

[19] Digital Intermediate Frequency Interoperability (DIFI) Consortium, "Website." [Online]. Available: https://dificonsortium.org

[20] S. Erwin, "Blacksky, maxar, planet win 10-year nro contracts for satellite imagery," *SpaceNews*. [Online]. Available: https://spacenews.com/blacksky-maxar-planet-win-10-year-nro-contracts-for-satellite-imagery/

[21] Kongsberg Satellite Services, "Ksat expands agreement to deliver ground station as a service related to reception of data from earth observing satellites with mnok280." [Online]. Available: https://www.kongsberg.com/newsandmedia/news-archive/20202/ksat-expands-agreement-to-deliver-ground-station-as-a-service-related-to-reception-of-data-from-earth-observing-satellites-with-mnok-280/

[22] N. Boschetti, N. G. Gordon, and G. Falco, "Space cybersecurity lessons learned from the viasat cyberattack."

[23] Defence Innovation Unit. Initial contracts for hybrid space architecture program. [Online]. Available: https://www.diu.mil/latest/developing-the-internet-of-space

APPENDIX

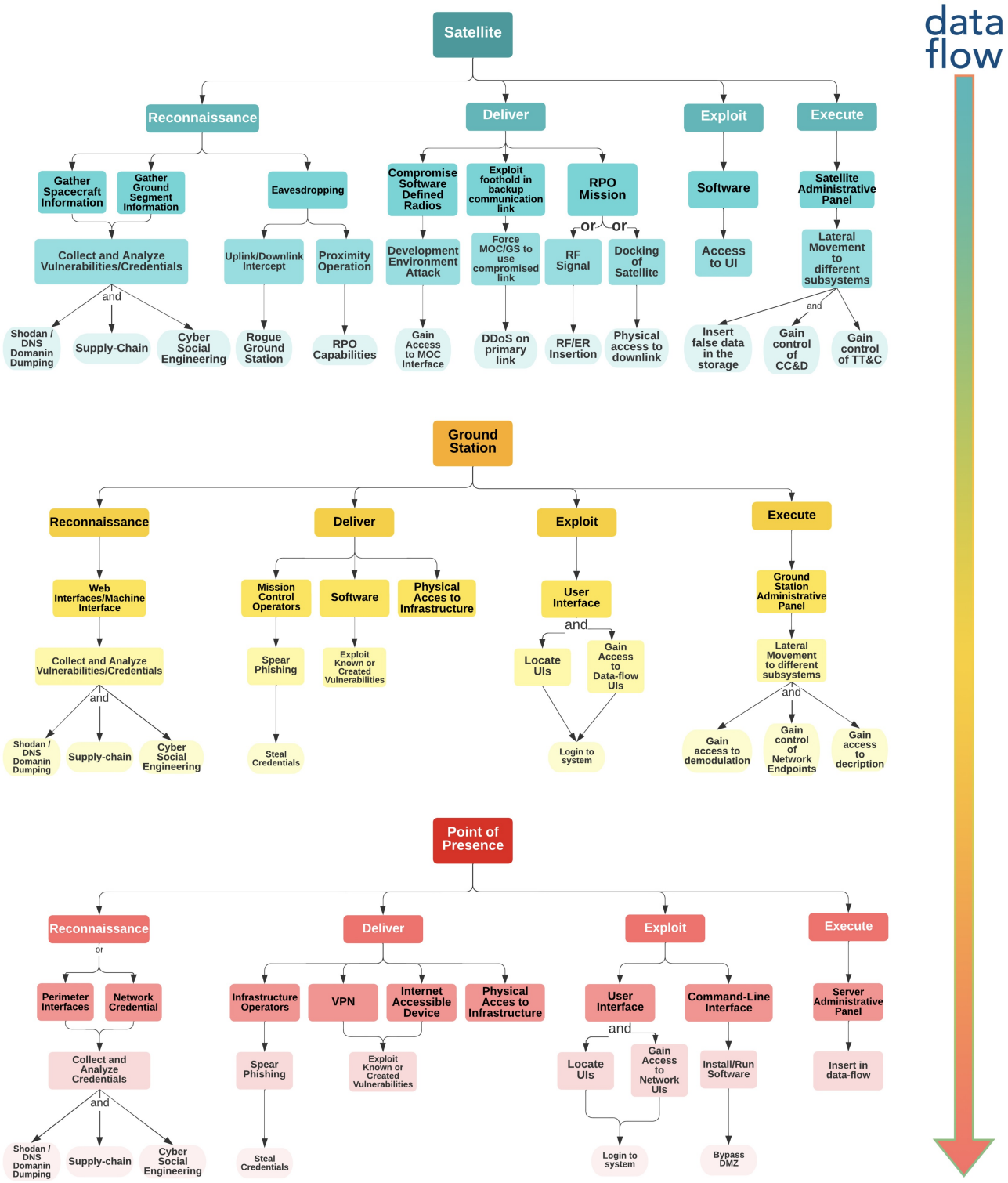

Figure 5: Full Architecture Attack Tree for False Data Injection Goal - Part I

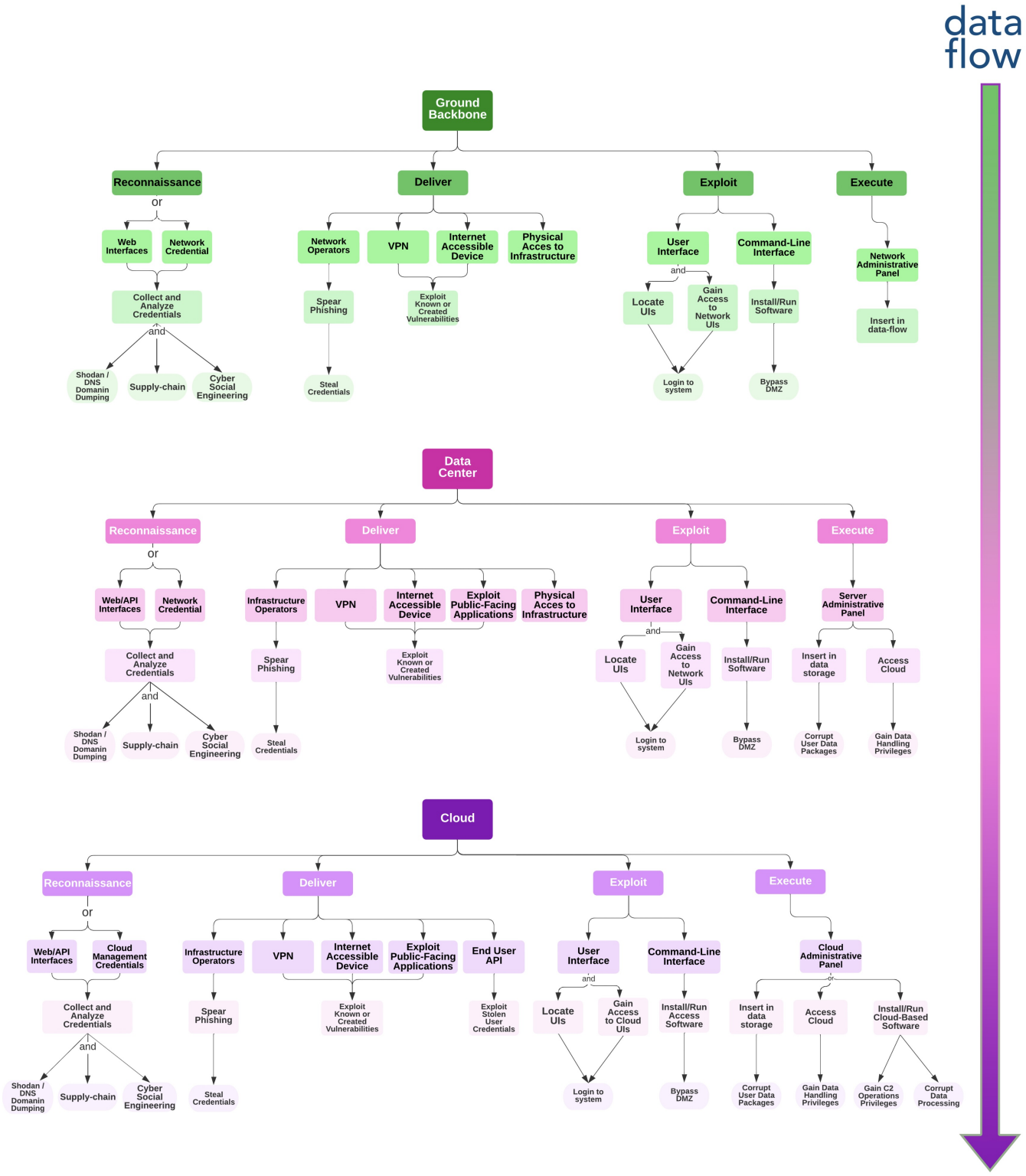

Figure 6: Full Architecture Attack Tree for False Data Injection Goal - Part II

BIOGRAPHY

Nicolò Boschetti *is pursuing a Ph.D. in Civil and System Engineering at the Johns Hopkins University and is an assistant researcher at the Aerospace ADVERSARY Lab at the JHU's Civil and Systems Engineering Department. He received his B.A. Degree in International and Diplomatic Sciences from the University of Bologna and his M.A. Degree in Politics and Economics of Eurasia from the Moscow State Institute of International Relations (MGIMO). His research focuses on the security of space systems, space cybersecurity, and the Russian space program and policy.*

Chelsea Smethurst *leads Microsoft's public policy related to enhancing resiliency and secure adoption for cloud security, critical infrastructure protection and commercial space systems. She represents Microsoft on the President's National Security Telecommunications Advisory Committee, the Cyber Readiness Institute, and several CISA public-private partnership forums. Prior to joining Microsoft, Chelsea worked for PwC and Deloitte delivering cloud security strategy and program solutions across Fortune 500 companies and the public sector. She's also worked for the U.S. State Department and at the Florida Attorney General. Chelsea has a BA in International Studies from University of South Florida, an MA in Global Affairs from Florida International University.*

Gregory Epiphaniou *currently holds a position as an Associate Professor of security engineering at the University of Warwick. His role involves bid support, applied research and publications. Part of his current research activities is formalised around a research group in wireless communications with the main focus on crypto-key generation, exploiting the time-domain physical attributes of V-V channels. He has also contributed to numerous public events and delivered keynotes around cybersecurity, course development and practical training to both private and government bodies. He was previously holding a position as a Reader in Cybersecurity and acted as deputy director of the Wolverhampton Cybersecurity Research Institute (WCRI).*

Carsten Maple *is Professor of Cyber Systems Engineering at the University of Warwick's Cyber Security Centre (CSC). He is the director of research in Cyber Security working with organisations in key sectors such as manufacturing, healthcare, financial services and the broader public sector to address the challenges presented by today's global cyber environment. He was previously Professor of Applicable Computing and Pro Vice Chancellor (Research and Enterprise) at the University of Bedfordshire. He has published over 200 peer reviewed papers and is co-author of the UK Security Breach Investigations Report 2010, supported by the Serious Organised Crime Agency and the Police Central e-crime Unit.*

Johan Sigholm *is an assistant professor at the Swedish Defense University and holds the rank of lieutenant colonel in the Swedish Air Force. His previous research has been focused on secure tactical communications, threat intelligence, and cyber operations. Dr. Sigholm received his M.Sc. in Computer Science and Engineering from Linköping University, and his Ph.D. in Informatics from the University of Skövde. He spent two years 2018-2019 as a Fulbright Postdoctoral Fellow at Harvard Kennedy School's Belfer Center and at MIT Sloan School in Cambridge, MA.*

Gregory Falco *is an assistant professor at the Johns Hopkins University in the Department of Civil and Systems Engineering and the Institute for Assured Autonomy, where he holds an appointment at the Applied Physics Laboratory in the Asymmetric Operations Sector. He is the director of the Aerospace ADVERSARY Lab that designs and develops autonomous and secure space infrastructure. His research entitled Cybersecurity Principles for Space Systems was highly influential in the development of Space Policy Directive-5, which shared the same title. He has been listed in Forbes 30 Under 30 for his inventions and contributions to critical infrastructure cyber security, is a Fulbright Scholar and is the recipient of the DARPA RISER and DARPA's Young Faculty Award. Falco completed his PhD at MIT's Computer Science and Artificial Intelligence Laboratory, Master's degree at Columbia University and Bachelor's degree at Cornell University.*