FFI Norwegian Defence Research Establishment

24/01118

FFI-RAPPORT

The cyber dimension of space systems

– an analysis of offensive cyber operations targeting space infrastructure

Ingunn Helene Landsend Monsen

The cyber dimension of space systems
– an analysis of offensive cyber operations targeting space infrastructure

Ingunn Helene Landsend Monsen

Norwegian Defence Research Establishment (FFI) 12 December 2024

Keywords
Romdomenet
Cyberdomenet
Satellitter
Rominfrastruktur
Cyberoperasjoner

FFI report
24/01118

Project number
1640

Electronic ISBN
978-82-464-3572-5

Approvers
Torgeir Mørkved, *Research Manager*
André Pettersen, *Research Director*

The document is electronically approved and therefore has no handwritten signature.

Copyright

Summary

Cyber security and space security are merging due to increased digitalization of space infrastructure and operations. Non-kinetic counterspace capabilities such as cyber operations are an attractive alternative to kinetic weapons due to their ability to avoid hazardous debris and operate below the threshold of armed conflict. This continued intertwining of outer space and cyber space introduces a larger cyber dimension to space infrastructure. This report is a step towards building an understanding of what this development may entail by exploring how offensive cyber operations can be used to target space infrastructure. It serves as a starting point for understanding the implications of these developments for security and strategy.

The research question guiding the analysis is “how does the space-cyberspace nexus influence the risk of offensive cyberoperations targeting space infrastructure?” The question is answered by analyzing how a motivated actor can gain access to key components of the infrastructure and what effect such operations may create. The analysis begins with a description of the elements of space infrastructure before expanding on a conceptualization of offensive cyber operations derived from cyber conflict literature. Further, we analyze how offensive cyber operations may be used to target space infrastructure. Focus is on two of the three components in space infrastructure: the ground segment and the space segment. Finally, we present a summary of effects and a categorization of vulnerabilities, before concluding and pointing to recommendations.

We identify two interlinked groups of vulnerabilities. The first is the vulnerabilities following from the practices in the contemporary space industry popularly called *New Space*. The second group of vulnerabilities follow from the lack of implementation of well-known best practices in ensuring adequate cyber security. The reasoning for these not being implemented is twofold. Firstly, there are practical challenges stemming from the physical qualities of space technology and infrastructure. Secondly, the New Space industry is still in its youth and has yet to establish a security culture incorporating an understanding of the cyber threat landscape. The limited attention allotted to cyber security responsibilities and risk in the supply chain of the space industry is a testament to this reality. This points to a need to prioritize an adequate risk awareness, security culture and cyber security in space systems.

We recommend strengthening the security and resilience of space infrastructure against offensive cyber operations by promoting comprehensive risk assessments, enhancing cyber security practices, cultivating a robust security culture, improving supply chain security, and enhancing preparedness through contingency planning and scenario-based implication analysis.

Sammendrag

Cybersikkerhet og romsikkerhet møtes som følge av den økte digitaliseringen av rominfrastruktur og -operasjoner. Ikke-kinetiske offensive romvåpen, som cyberoperasjoner, er et attraktivt alternativ til kinetiske romvåpen på grunn av evnen deres til å unngå skadelig romsøppel og fordi de enklere kan brukes under terskelen for væpnet konflikt. Denne rapporten skal bidra til å styrke forståelsen av hva cyberdimensjonen i rominfrastruktur kan føre med seg, ved å utforske hvordan offensive cyberoperasjoner kan rettes mot ulike deler av rominfrastrukturen. Rapporten skal fungere som et utgangspunkt for å forstå konsekvensene av utviklingen for sikkerhet og strategi.

Forskningsspørsmålet for analysen er: «Hvordan påvirker sammenflettingen av rom- og cyberdomenene risikoen for offensive cyberoperasjoner mot rominfrastruktur?» Spørsmålet besvares ved å vise hvordan en motivert aktør kan få tilgang til nøkkelkomponenter i infrastrukturen, og hvilke følger operasjonen kan forårsake. Analysen starter med å beskrive standardkomponentene i rominfrastruktur. Deretter presenteres en konseptualisering av offensive cyberoperasjoner basert på litteratur fra cyberkonfliktstudier. Videre kombineres disse to i en analyse av *hvordan* offensive cyberoperasjoner kan rettes mot bakkesegmentet og romsegmentet i rominfrastruktur. Til slutt oppsummeres mulige effekter og en kategorisering av sårbarheter, før konklusjon og anbefalinger presenteres.

Gjennom analysen identifiseres to sammenkoblede grupper sårbarheter. Den første gruppen følger av praksis og i dagens romindustri som populært kalles *New Space*. Den andre gruppen sårbarheter skyldes manglende implementering av velkjente prosedyrer for å sikre tilstrekkelig nivå av cybersikkerhet. Grunnen til at disse ikke er implementert, er todelt. For det første finnes det praktiske utfordringer knyttet til fysiske egenskaper ved romteknologi og -infrastruktur. For det andre er *New Space*-romindustrien fortsatt ung og har ennå ikke etablert en sikkerhetskultur som inkorporerer en god nok forståelse for cybertrusler. Den begrensede oppmerksomheten som er viet cybersikkerhetsansvar og -risiko i industriens forsyningskjeder, understreker dette. Disse utfordringene peker på behovet for å prioritere tilstrekkelig risikobevissthet, sikkerhetskultur og cybersikkerhet i romsystemer.

De anbefalte tiltakene er ment å styrke sikkerheten og motstandsdyktigheten i rominfrastruktur mot offensive cyberoperasjoner gjennom å fremme omfattende risikovurderinger, forbedrede cybersikkerhetspraksiser, en robust sikkerhetskultur, forbedret sikkerhet i forsyningskjeder og forberedelse gjennom beredskapsplanlegging og scenariobasert implikasjonsanalyse.

List of abbreviations

ADCS:	Altitude determination and control system
ASP:	Arctic Surveillance Program
ASBM:	Arctic Satellite Broadband Mission
COTS:	Commercial of the shelf systems
CSpO:	Combined Space Operations initiative
CYFOR:	Norwegian Cyber Defense Forces
C&DH:	Control and data handling
DBS:	Norwegian Directorate for Civil Protection
ESA:	European Space Agency
FMR:	Official Recommendation from the Chief of Defense
FOH:	Norwegian Joint Headquarters
GEO:	Geosynchronous orbit
GNSS:	Global Navigational Space Systems
GPS:	Global Positioning System
TT&C:	Telemetry, tracking and control
HEO:	Highly elliptical orbit
IP:	Internet Protocol
ISR:	Intelligence, surveillance and reconnaissance
ITU:	International Telecommunications Union
JPL:	The Jet Propulsion Lab
KDA:	Kongsberg Defense and Aerospace
KSAT:	Kongsberg Satellite Services
LEO:	Low earth orbit
LTP:	Long term plan for the defense sector
MEO:	Medium earth orbit
NFD:	Norwegian Ministry of Trade, Industry and Fisheries
NIS:	Norwegian Intelligence Service
NOAA:	National Oceanic and Atmospheric Administration
NRS:	Norwegian Space Center
NSM:	Norwegian National Security Authority
PNT:	Position, navigation and timing
RF:	Radio frequency
SATCOM:	Satellite Communication
SDA:	Space Domain Awareness
SJ FOH:	Chief of the Norwegian Armed Forces' Operational Commando Center
SSN:	Space Surveillance Network
TCP:	Transfer Control Protocol
VSAT:	Very small aperture radar

List of figures

Contents

Preface

This research has been conducted under the auspices of the FFI project "Technological trends with implications for Norwegian military operations" (Tekno). The Tekno project adopts a long-term focus regarding the potential implications of emerging and disruptive technologies (EDTs). Space technology is one of these EDTs, along with artificial intelligence, autonomy, quantum technologies, additive manufacturing, synthetic biology, soldier enhancement systems, hypersonic vehicles, materials sciences, among others.

This report is an exception to the typical approach of the Tekno project in that it deals primarily with current technology instead of future trends. Digitalization trends, and the increased interconnectedness that results from this digitalization, is nevertheless a highly relevant aspect of emerging technologies and one that heightens the relevance of the cyber dimension for all EDTs as time progresses. By focusing solely on the cyber dimension in space infrastructure as it appears today, this report serves as an analytical steppingstone to understanding the implications of an expanding cyber dimension in all technologies on the future battlefield.

In addition to understanding the content and projection of the EDTs, the aim of our work at Tekno is also to explore how future technology may be used in military operations. This study deals with mature technology but focuses on a mode of offensive use of which there is little empirical experience to date. As such, it contributes to show the potential impact of this type of offensive capability.

At Tekno, we are fortunate to be able to lean on the expertise of the many research areas represented at FFI to enhance the technological understanding in our analyses. The work behind this report is no exception. The guidance and input from the space research group at FFI, headed by Richard Olsen, has been indispensable for the sections on space infrastructure and the Norwegian Space Program. I have also received valuable input from the cyber research group at FFI and researchers within the field at other national institutions. The discussions and feedback provided by colleagues are greatly appreciated and have contributed to enhancing the quality of the research.

Kjeller, 25.09.2024

Ingunn Helene Landsend Monsen

1 Introduction

One hour before Russia began its full-scale invasion of Ukraine on February 24th, 2022, Ukrainian users of the ViaSat's KA-SAT broadband network lost contact with the service. The Ukrainian army was one of ViaSat's customers. The offensive cyber operation behind this event began with an intrusion through a VPN-service, before the attackers entered the management segment of the user terminals and deployed the wiper malware Acid Rain on the users' modems. This rendered between 40.000 and 45.000 of them inoperable, affecting Ukranian, as well as other European customers (Greig, 2022, 2023; Splunk Threat Research Team, 2022).[1] The ViaSat-hack has put the cyber vulnerabilities of space systems on the agenda and contributed to an emerging understanding of the vulnerability of these systems.

The digitalization of societies and military systems has created a new type of target that can be exploited. An actor may gain remote access to computer systems and monitor, steal, destroy or manipulate data or system processes and functions. The digitalization trend includes infrastructure connected to space systems and introduces a cyber dimension to space infrastructure. The security norm in space technologies has typically been *security through obscurity*, referring to an assumption that the physical distance and technological sophistication of systems in orbit are so challenging to overcome that other security measures seem unnecessary.[2] The contemporary space sector is now fundamentally changed from the early space age when this was the norm. Today, it is filled with a plethora of actors, sunk cost and democratized access to the technology and domain. Nevertheless, the cyber security of space infrastructure was for a long time underprioritized.[3]

Outer space and cyberspace share qualities that give them particular strategic value such as geographical reach and enhanced scale of intelligence collection through either overhead placement or globally connected information systems (Livingstone & Lewis, 2016; Martin, 2023). The two domains have commonalities in that they hold unresolved geopolitical tensions (Fidler, 2018). None of the great powers have to date agreed on how to approach either cyber security or military activity in outer space (Robinson, 2016).[4] The lack of established norms, clear red lines and relative anonymity when conducting cyber- or space operations lead to good conditions for covert malicious activity. An initial step in unpacking what this means for security is to understand how the two domains are combined in space infrastructure, and how this creates opportunities for malicious targeting with offensive cyber operations.

[1] See (Boschetti et al., 2022; Poirier, 2022) for a more in depth analysis.

[2] This norm was established when there were but a few spacefaring nations that possessed the technology and knowhow to conduct space operations.

[3] This statement has been echoed by many scholars in the technical field, as will be revisited in later sections of this report.

[4] The Outer Space Treaty from 1967 is the central legal framework that regulates state behavior in outer space. The treaty states some norms and rules but is silent or open for interpretation on several important topics such as weapons in orbit, and do as all international legislation carry weak enforcement mechanisms (United Nations Office for Outer Space Affairs, 1967).

The aim of this report is to aid in advancing the understanding of what the continued intertwining of space infrastructure and cyber space may entail for security and strategy. To achieve this aim, this research will answer the overarching question "how does the space-cyberspace nexus influence the risk of offensive cyberoperations targeting space infrastructure?" Risk is understood as the function of two factors: the *probability* of an event occurring, and the *impact* or consequences. The analysis clarifies the scope of risk by exploring the technological underpinnings of the space-cyberspace nexus and the avenues for exploitation using offensive cyber operations.

1.1 The merging of two security domains

The fields of cyber security and space security are merging as a function of several developments that have evolved gradually over the past decades. The developments are connected to culture and industry, strategic context, and some are tied to the space technology itself. Space infrastructure has become increasingly digitalized over the years (Poirier, 2022). The digitalization is imbedded throughout the different phases of technology development, from design through testing, as well as during the conduct of operations (Department of the Army, 2014). There is an increase in the usage of software defined radios, IP-protocols, and increased on-board processing (Poirier, 2022). What before was determined by physical hardware is now increasingly software defined. This entails that the digital aspects of space infrastructure have become more important to their functionality and operation (Poirier, 2022).

There have been structural and cultural changes to the industrial ecosystem of space technologies as well. *New Space* is a term used to describe the change from a space industry dominated by a few state-run companies to a new economic ecosystem with several smaller actors. New space industry has opened for private financing models, commercial technology development, and over time has increased ease of access into orbit, lowering the bar for new industries and services in the domain (Brockmann & Raju, 2022, pp. 4–5; Paikowsky, 2017).[5] As we are currently experiencing the first wave of this trend, scholars are highlighting the many cyber security challenges currently unaddressed in this ecosystem (Falco, 2018; Fidler, 2018; Livingstone & Lewis, 2016; Manulis et al., 2021; Pavur & Martinovic, 2022). Some authors have pointed to a *digital conundrum* taking place where on the one hand, the digitalization of space systems makes them more vulnerable to traditional cyber threats, demanding the adaptation of traditional cyber security measures. On the other hand, the unique nature of space systems often renders traditional cyber security inadequate (Pavur & Martinovic, 2022; Poirier, 2022). There are several reasons for this, which will be expanded on further in section four.

The intersection of the space- and cybersecurity domains are receiving more attention in some segments of the security and technology research communities. Traditionally, Space security literature has been preoccupied with kinetic threats such as space weapons, hazardous debris, anti-satellite weapons (ASATs) and physical threats from outer space (Johnson-Freese, 2017;

[5] In 2012, a total of 134 objects were launched into orbit. Ten years later, in 2022, the number was 2163 (Our World in Data, n.d.).

Klein, 2019). However, there has been a surge in research on non-kinetic counterspace operations in the later years (Swope, 2024; Bingen, 2023; O'Connor, 2022; Rajagopalan, 2019; Prague Security Studies Institute, 2018). Non-kinetic counterspace capabilities, such as cyber operations offer positive cost benefit ratios for adversarial states. Firstly, they do not lead to the spread of hazardous debris, as do kinetic attacks. Since all modern states rely on space services for economic, military and societal activity, using a method that may target your adversary but not threat one's own space services would be preferable. And secondly, in an era of global strategic competition, there are benefits to keeping one's own offensive activity under a threshold that might trigger an open military response. Such *sub-threshold*-activities allow states to robustly compete to achieve relative gains without triggering a direct military confrontation (Kaushal, 2021). Therefore, using methods that are harder to attribute and not explicitly comparable to kinetic attacks, such as cyber operations, are an attractive option.

Both outer space and cyberspace are warfighting domains which entails that they are organizationally included in military capability building and strategy (Dolman, 2022, p.85). We have become accustomed to offensive cyber operations of varying severity targeting companies, private individuals and public agencies. States in competition or conflict are regularly using offensive cyber operations as a tool to steal information from, confuse or undermine their adversaries. Researcher Clémence Poirier has pointed out that the continued intertwining of cyber space and outer space is leading to the elevation of the offensive activity we see within the militarized cyber space into orbit (Poirier, 2022). This may mean that the cyber operations we have grown accustomed to as a daily occurrence in the terrestrial information systems may become more relevant for space systems.

The cyber and space domains are combined through the role of space assets in maintaining global internet connectivity. Firstly, timestamping-services provided by global navigational satellite systems (GNSS), such as GPS and Galileo, play a vital part in providing affordable synchronization of internet services globally.[6] Secondly, direct broadcast services from satellites in geosynchronous orbit (GEO) have from the advent of direct-to-consumer space services been the most widely used type of space technology. In the later years, there has been a shift to broadband-satellites stationed in low earth orbit (LEO) (Poirier, 2022). Terrestrial cables have traditionally been the backbone of internet infrastructure but are now being supplemented by internet services from constellations of satellites. Companies like Starlink, OneWeb, Blue Origin and Virgin Galactic are steadily launching microsatellites that hold the promise of providing high speed internet to areas of the world with little ground-based infrastructure (Brunkard, 2021). Looking forward, this trend points to a growing dependency on space infrastructure for upholding global internet coverage.

[6] Timestamping is used to record precisely when an event is recorded by a computer system. This function is crucial for effective communication between networked computers and applications through the internet (Lutkevich, 2021).

1.2 Limitations and report structure

Several factors limit the analysis in this report. Firstly, the focus is on space operations using satellites orbiting the earth. There are several deep space missions and scientific endeavors from both the International Space Station (ISS) and its Chinese counterpart, the Tiangong Space Station. These will all be omitted in the following discussions to limit the scope of the study.

The literature on the New Space ecosystem underpinning this research does not distinguish between military and civilian systems and actors. I will do the same in this study but include an assumption that the military systems carry additional protections. It is worth noting that distinguishing civilian from military activity and systems in this ecosystem is not straightforward. The New Space-industry consists of many civilian private actors, but also includes smaller non-traditional spacefaring nations and their military endeavors. Many satellites are designed to be *dual-use* with separate military and civilian systems on board. Additionally, many states highlight the importance of civil-military cooperation in space capabilities, which further obscures the division. As a result, the relative sizes of the civil versus military infrastructure and systems is difficult to define. Ultimately, the distinction is less relevant when it comes to offensive cyber operations, seeing that they are typically used against both types of targets.

The research question guiding this report is "how does the space-cyberspace nexus influence the risk of offensive cyberoperations targeting space infrastructure?" Risk is understood as the function of two factors: the *probability* of an event and its *impact* or consequences. The analysis builds on a review of the literature at the intersection of cyber security and space security. It combines technical scholarship with the branch of security studies scholarship that focuses on the impact of technology on international security.

The research question will be treated in a two-steps. First, I will describe how cyberspace and space infrastructure are intertwined from a technical standpoint. I begin by describing the underlying technology of space systems in section two before I discuss the relevant components and qualities of military cyber operations in section three. A brief analysis of how to understand cyberspace within space infrastructure is conducted in this here. Section four will fulfill the second step and main analysis component of this report by applying the conceptualization of offensive cyber operations onto components of the space infrastructure. For simplicity, focus is put on two of the three components of space infrastructure: the ground and space segments.

This analysis will incorporate the factors of *how* an actor can gain access with an offensive cyber operation and *what* effect it can cause. This will be exemplified with vulnerabilities highlighted in the literature on space-cyber security, as well as empirical evidence and technical analyses showing proof of concept. The analysis will serve as a non-exhaustive overview of how offensive cyber operations may be used to target space infrastructure. After briefly summarizing the analysis, I offer recommendations and sum up the results of the research conducted in a concluding section.

The analysis is intended to be general and does not have a particular national focus. However, I introduce a link to Norway through information boxes on the Norwegian Space Program, satellite fleet and Norwegian definitions and organizational approaches to cyber operations. These are intended as a supplement to the main conceptual analysis. The link to Norway is brought forward again in the final section where recommendations with relevance for Norway are highlighted.

2 Space infrastructure

The following section will expand on the underpinning technology of space systems and touch on the operations conducted in the domain.

Space infrastructure is typically divided into three main segments.

- A ground segment which maintains the control center and ability to send and receive signals from the system in orbit. In broader definitions, the facilities and industry for technology development and launch are also included in this structure (Manulis et al., 2021, p. 289). This includes the systems design and testing of the launch vehicles and satellites.

- The space segment, which is typically placed in one of four types of orbits; Low earth orbit (LEO), medium earth orbit (MEO), geosynchronous orbit (GEO), or a highly elliptical orbit (HEO).[7] This can be one satellite or a constellation of multiple satellites.

- The user segment is located where the services provided by the system are disseminated. This can be an Internet service provider, further distributing internet connectivity through its ground infrastructure, or customer terminals for military communications.

[7] LEO is defined as reaching up to around 2000 kilometer above the earth's surface, and objects here reach a speed of about 8km/s. MEO stretches from the upper LEO border until just below the limit for GEO, which is at approximately 35 000 km altitude. The GEO-satellites move with a speed of 4 km/s, which corresponds to the earths turning. The inclination of the orbit can vary and influences which areas are covered. The GEO-satellites directly above the equator have continuous coverage of the direct below area, called *geostationary* orbit (Bjerke & Olsen, 2008, pp. 15–18) Highly elliptical orbit is not precisely defined, but refers to when a orbit is close to the earth at one point, and have an apogee (highest point) under 45 000 km.

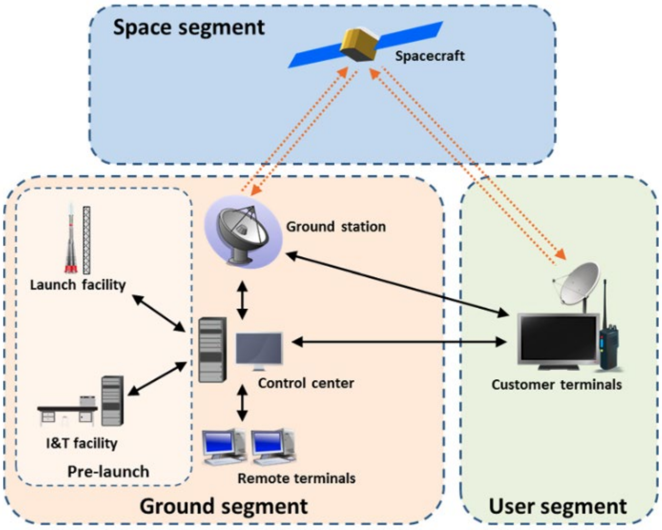


Figure 2.1 The central components of space infrastructure. (Manulis et al., 2021)

Satellites conduct a wide array of different functions and are placed in orbits that provide the best conditions for their tasks. Earth observation satellites using optical sensors stay in a sun-synchronous orbit where they may constantly use sunlight to illuminate the earth's surface. Satellites in low earth orbit have short overflight times but high fidelity of signal because of their proximity to the earth. These characteristics make low earth orbit ideal for communications and internet satellites. The further away from earth an asset is, the higher latency there will be on the signal. By contrast, the speed of orbiting objects is much higher closer to earth than further away. There is therefore a tradeoff between latency and continuity of services (Bjerke & Olsen, 2008). Space segments in geostationary orbit travel at the same speed as the earth and provide continuous coverage of the area the signal can reach. The curvature of the earth's surface places this limit at approximately 65-70 degrees north and south.[8] Typical services provided from GEO are from large broadcasting services, communication satellites, meteorological satellites, and military early warning systems. Most satellites used for positioning, navigation and timing (PNT), such as GPS, Glosnass and Beidou, are placed in MEO and maintain continuous services by having many assets in orbit. Services needed for the areas nearing the poles will make use of polar orbits. These span from earth observation, communication, and PNT-services (Thorpe, 2022).

2.1 Ground segment

The ground segment consists of the infrastructure needed to monitor and control the satellites' orbit and payload activities, and the ability to disseminate the received signals to other systems.

[8] Topography and vegetation can affect the actual coverage.

The ground station is one component in the ground segment that may, in its most stripped-down form, consist of a computer with mission control software and a radio frequency (RF) sender/receiver. In larger networks, the ground segments can be dispersed over larger distances with terrestrial communication connection to each other (Manulis et al., 2021, p. 289; Pavur & Martinovic, 2022).[9] It is the orbit in which the space segment operates that dictates where the ground station should be placed. The signal connecting the satellite and ground station travels in a straight line, and the curvature of the earth and the satellite's distance to the earth dictates where the signal from the satellite can reach. Satellites in polar orbits have inclinations nearing 90 degrees from the equator to be able to cover the polar regions. The ground stations servicing these orbits will need to be placed in areas that can achieve contact with these satellites. The satellite ground station on Svalbard is located at 78 degrees north to be able to connect with satellites in polar orbits.

2.1.1 Space surveillance infrastructure

Part of the terrestrial infrastructure needed for space operations is the Space Surveillance Network (SSN), which is a global surveillance system covering and tracking all objects in orbit of the earth down to 10 cm in size in LEO and approximately one meter in GEO (Sgobba & Allahdadi, 2013). Each satellite operator has control over the trajectory of their own asset, but they rely on SSN to understand how their asset moves in relation to the other orbiting objects. The system is operated by the United States Space Force and consists of a catalogue of all tracked objects in orbit and a surveillance infrastructure consisting of ground and space-based sensors. The sensors include conventional radars, phased-array radars, electrical-optical sensors and a "The Midcourse Space Experiment" satellite, which carries a range of sensors in orbit and feeds data into the surveillance network (Sgobba & Allahdadi, 2013).

The data from this system is what most space actors rely on for *Space Domain Awareness* (SDA). SDA is knowledge about the activity in the space domain including trajectories of one's own and other objects in orbit (Sgobba & Allahdadi, 2013). There are currently 8,600 operational humanmade objects orbiting the earth and approximately 34,670 pieces of space debris up to 10 cm in size and one million sized between one and 10 cm. 130 million fragments are smaller than one cm in size (European Space Angency, n.d.).[10] Other states and the European Union are working to build up their own infrastructure for this aim, but the US SSN remains the most advanced.[11] This tracking data and the infrastructure that underpins it is an important part of ensuring the safety of one's space asset through avoiding collisions.

[9] The ground station, which receives and transmits the RF-signal to the space segment, can be remotely located from the control segment and other remote satellite terminals, although the ground station and control center often are grouped together.

[10] "Near-Earth space is cluttered with some 36,500 pieces of space debris larger than 4 inches (10 centimeters), about a million objects 0.4 to 4 inches (1 to 10 cm) in size, and an astounding 130 million fragments smaller than 0.4 inches (1 cm).» (European Space Angency, n.d.)

[11] For example, China has been working to establish its own infrastructure, which needs to be distributed across the globe in order to obtain the needed coverage of space. (Singer & Wood, 2021) The European Space Agency is also in the process of building up its own catalogue of objects in orbit (The European Space Agency, n.d.).

2.2 Space segment

The space segment is the component of space infrastructure that is placed in outer space. Although most space segments today are satellites, manned space stations such as the ISS are also included in this category. A satellite has several typical characteristics. It has a casing designed to withstand the harsh environmental conditions of outer space such as radiation, as well as vibrations and shock loads during launch. Solar panels provide energy for systems function, accompanied by a battery. Many satellites have onboard fuel and a propulsion engine to adjust their own orbits, either for mission requirements, or for evasive maneuvers if debris is on a collision course. Within the satellite, there is a payload, which delivers the service for which the system is put in orbit.

The command and data handling system (C&DH) decodes and validates a received signal and distributes it to the relevant sub-system. This includes tasks from the ground segment regarding the payload or the operating system of the satellite. It may be updating and adding components to the operating system or tasking the satellite to alter its orbit ("Components of a Satellite," n.d.; Manulis et al., 2021). If an error occurs in the space segment, the command system is the only option to either correct or circumvent the error. It is therefore a critical point in the system (Bjerke & Olsen, 2008, p. 14). The attitude determination and control system (ADCS) senses whether the satellite is in the correct orientation in orbit and can be commanded to correct this when needed.

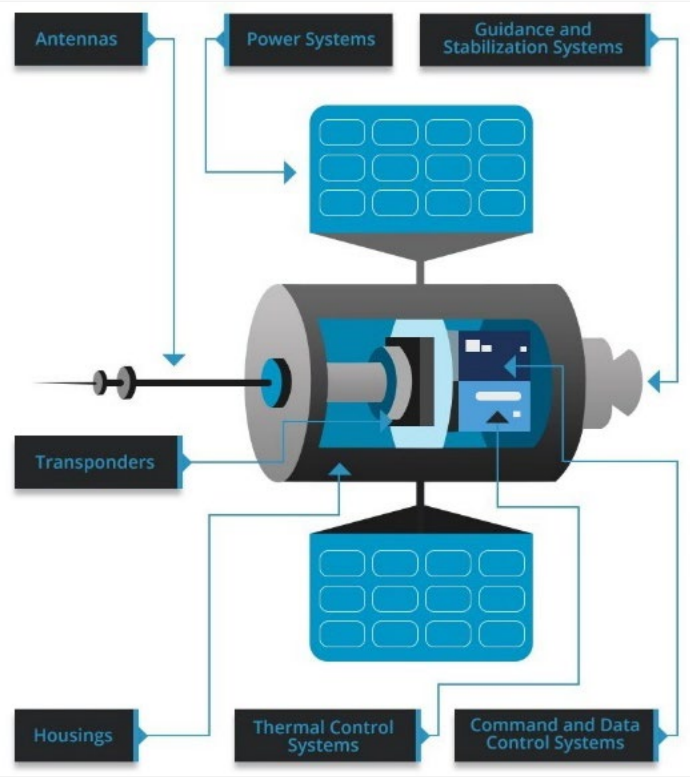

Antennas
Power Systems
Guidance and Stabilization Systems
Transponders
Housings
Thermal Control Systems
Command and Data Control Systems

Figure 2.2 The standard components of a satellite. ("Components of a Satellite," n.d.)

Today, most satellites are equipped with a GPS receiver for determining a satellite's position in orbit. The GPS is also frequently used as a timing reference for timestamping collected data or synchronizing other functions onboard the satellite. And finally, the antennae and transponder combine to the telemetry, tracking and control function (TT&C) which create an interface between the ground and space segments in that it receives and processes the uplink, from the ground to the space segment, and downlink signals returning from space to the user segment ("Components of a Satellite," n.d.; Manulis et al., 2021, p. 289).

2.2.1 Payloads

The above components are standard to most satellites regardless of type and service provided. Satellite payloads can vary and are broadly categorized according to the types of services they provide. Smaller categories, such as the different instruments for scientific research or technology demonstration payloads, are excluded here for the sake of simplicity.

Communication services include satellite telecommunication, television broadcast, and data communication. In the latter category, very small aperture terminals (VSATs) are used to send data from one point to another. Internet service providers are becoming the largest customers in this field. Overall, the communication services make use of satellites as a mirror to transport signals through space for the sake of increased reach. The payload in these types of satellites is the communications equipment that allows receiving and transferring signals (Bjerke & Olsen, 2008). PNT-services aids a signal receiver to calculate its location, navigate and give precise timestamping of events (Thorton, 2023). The different GNSS systems, such as Galileo, GPS and Beidou are examples of such services. The payload on PNT-satellites is the PNT signal generator and its transmission equipment (Bjerke & Olsen, 2008). Newer designs include software defined signal generators (Northorp Grumman, 2021).

Earth observation and remote sensing services encompass several civil and military types of services that use the space segment to collect data. These types of payloads are plentiful and are divided into active and passive sensors.[12] The former category provides its own energy source in order to actively detect or observe the objects they search for, whereas passive sensors do not actively send signals and interpret what is received, but rather detect the energy that is released or reflected from its target (Earth Science Data Systems, 2022). There are a plethora of different sensors that are in use for remote sensing from space. Examples include infrared sensors measuring heat signatures, optical sensors that collect imagery, radar and lidar-sensors detect and measure distance to objects, and hyperspectral sensors that collect more detailed information from the earth's surface through the electromagnetic spectrum (Critchley, 2018).

All sensory inputs go through at least some on-board-processing before being transmitted to the ground or user segment. A primary reason is to limit the use of capacity on the signal link, which is a limited resource. The processing on a satellite is often limited because of space and weight limitations, inability to update hard- and firmware, and limited power availability (Bjerke & Olsen, 2008).[13] At the most basic, the computers will have to manage the minimum capability of maintaining the correct altitude, keep its antennae in the necessary position, and its solar panels tilted in the correct direction for solar rays absorption (Bjerke & Olsen, 2008). This

[12] NASAs websites the number of types of sensors on board NASA-operated satellites amount to over a hundred (Earth Science Data Systems, 2022).

[13] Computers with high processing capacity emit heat as a biproduct, which is a challenge to regulate in the state of vacuum in which satellites operate. Therefore, the range of complexity and capability of the computing systems on satellites vary widely.

means that at a minimum, the digital components of a satellite are present in the 'survival functions' of telemetry[14], energy management and mission control, as well as what is the minimum needed for the payload.

The Norwegian satellite fleet

The Norwegian fleet of satellites currently consists of technology demonstrators and prototypes with maritime surveillance capabilities. AISSat-1 & 2, NorSat-1, 2, 3, 4 and TD were launched between 2010 and 2024 and carry different mixes of AIS-trackers, passive sensing- and data transfer- and communication payloads (Hofoss et al., 2023, pp. 20–21; Norwegian Space Center, n.d.). ARCSAT launched in 2022 is a research satellite exploring satellite communication (SATCOM) technology and concepts in the Arctic. The Birkeland and Huygens nanosatellites are a cooperation with the Netherlands that use formation flying and passive radar technologies for precise maritime surveillance. The twin satellites make up the MILSPACE-2 constellation, a pioneering project active in polar orbit (Norwegian Space Center, n.d.).

Many more satellites will join the Norwegian fleet within a few years. The Norwegian commercial company Space Norway has several ongoing projects for capability development. The HEOSAT-project is a constellation of two satellites dubbed the Arctic Satellite Broadband Mission (ASBM) that was launched from California in August 2024 (Space Norway, n.d. Erwin, 2024). This capability will provide continuous broadband coverage for users in the Arctic region and will have military and civilian customers, including the US Armed Forces (Eide, 2023, p. 25, Erwin, 2024).

Three constellations for maritime surveillance are currently in development which will be managed through a common operational concept by the commercial company Kongsberg Satellite Services (KSAT). MicroSAR is developed by Space Norway and will carry a synthetic aperture radar for maritime surveillance, with the aim of a constellation reaching between three and six assets. N3X is Kongsberg Defense and Aerospace's (KDA) latest version of the NorSat satellites and will carry an AIS tracker as well as a detector of navigational radars. Arctic Ocean Surveillance satellites are government-financed and developed in cooperation with ESA and NRS and will carry several sensors. It is projected that the Norwegian Armed Forces will be a main client of services from all three of these constellations (Hofoss et al., 2023, pp. 7, 20–21).

[14] Telemetry refers to the on-site collection of data or measurements typically at remote nodes in a system and their automatic transfer to a recipient. Telemetry on a satellite refers to the collection of data about the systems and situation on board the satellite and its automatic transfer to the ground station for monitoring (Birkeland, 2022).

2.3 User segment

The user segment is where the services provided by the satellite are received and used. It often has only a downlink capacity receiving signals from the satellite, in contrast to the ground station that can issue uplink-signals with commands. An exception is the case of satellite communication services where the user sends signals to a counterpart via the space segment. For internet satellites, the user segment is typically a terminal that receives the signal and disperses it further via other internet infrastructure (Manulis et al., 2021, p. 302). This segment is often left out in the vulnerability analyses in the literature on cyber security in space systems (Bingen et al., 2023; Falco, 2018; Livingstone & Lewis, 2016; Thangavel et al., 2022). This may be because malfunctions in this segment are less critical and restoring function is relatively easy given physical access to the infrastructure. However, the ViaSat KA-SAT operation in 2022 illustrates how this part of space infrastructure can be exploited with important consequences.

2.4 The signal

The contact to and from the space segment takes the form of radio frequency signals. Higher frequencies can send more data than lower frequencies, although they will need more energy to do so. The radio frequency (RF) bands used for satellite up- and downlink are typically the L, S, C and Ku (Fritz, 2013, pp. 2–3). These frequencies are coordinated by the UN agency International Telecommunication Union (ITU) (The International Telecommunication Union, n.d.). Digital communication uses Transfer Control Protocols/Internet Protocols (TCP/IP) which is “a set of standards that define how computer programs will break data up into packets, and send it across a data network to a specific device, which can output it” (Blount, 2017, p. 276). Satellites often use several layers of protocols and some of the most widely used are detailed in the “TM Space Data Linc Protocol” (The Consultative Committee for Space Data Systems, 2021). What is important to note is that the protocols themselves can be transported on a wide array of mediums (phone lines, cable lines, electromagnetic spectrum, or fiber optic cables), and in the case of satellites, they take the form of radio waves (Blount, 2017). An uplink signal begins with data being transferred through a modem, through an up-converter into a high-power amplifier and issued through an antenna (Fritz, 2013, p. 3). The uplink-transport sends a signal from a ground station to a space segment. The downlink from the satellite happens in the same way from the space segment. When the signal reaches the ground station through the antennae it travels through a low-noise-amplifier onto a down-converter. It continues to the control-computer through a modem and on to the customer (Fritz, 2013, p. 4). Encrypting the signal should ensure the security of the content of the transmission.

The Norwegian Space Program

The roots of the Norwegian space program reach back to the establishment of Andøya Rocket Range, where the first research rocket studying the ionosphere was launched in 1962 (Holtet & Hammerstrøm, 2023). Norway has from the outset fulfilled most of its military and civilian needs for space capabilities through different formats of international cooperation. Norwegian membership in the European Space Agency (ESA) dates to 1987 and has been an important arena for collaborative space projects. Norway has also participated in space technology and capability development through the EU and several bilateral formats.

The establishment of Program Space at the Norwegian Ministry of Defense in 2017 was a turning point in Norwegian military space history, where the space domain was introduced as an operational domain for the Norwegian Armed Forces (Olsen, 2017). Program Space was created after initiatives from the 2015 official recommendation from the Chef of Defense (FMR) and the long-term plan for the defense sector (LTP) from the following year. The program adopted an approach to developing space capabilities that should be moderate and conducted gradually over time.[15] The stated ambition was that it should be as civilian as possible, and as military as necessary (Norwegian Ministry of Defense, 2016; Norwegian Ministry of Defense, 2020, p. 109; Eide, 2023, p. 18; Norwegian Defense Staff, 2015).

National standalone space capabilities gained additional importance from 2019 when NATO declared outer space as an operational domain (NATO, 2022). A Norwegian ability to provide robust space-based services in the High North would be an important contribution to the Alliance (Norwegian Ministry of Defense, 2020, p. 109; Eide, 2023, p. 18). A national strategy for Norwegian space activity also arrived in 2019, and although it emphasized the commercial and societal importance of outer space, it illustrated the change of approach by including defense and security policy as one of four national strategic goals for the first time (Norwegian Ministry of Trade, Industry and Fisheries, 2019, p. 8).

Organization and way forward

The focus on Norwegian commercial interests in the 2019 strategy reflects the fact that the overarching responsibility for space matters lies with the Ministry of Trade, Industry and Fisheries (NFD). The Norwegian Space Center (NRS) is a central subordinate agency with responsibility for representing Norwegian interests in European (ESA and EU) and other international space cooperation formats. The NRS is also charged with managing the civilian national space budget and supporting commercial and public actors in space matters ranging from space policy to product and service development (Norwegian Ministry of Trade, Industry and Fisheries, 2006).

[15] Original terms are «nøktern» and «trinnvis», respectively.

The military organizational structure has been in development for some time due to long processes for landing on a doctrinal approach that marries the different military functions fulfilled through the domain.[16] The responsibility for developing and exercising military space activities is today divided along two lines under the Norwegian Chief of Defense. Firstly, the Norwegian Joint Headquarters (FOH) and Norwegian Intelligence Service (NIS) are equally positioned along one line. The NIS holds the domain authority[17] for military space operations and has operational responsibility[18] for ISR activities and Space Domain Awareness (SDA). The FOH is the Space Coordinating Authority (SCA) which entails integrating space capabilities in joint operations. FOH also maintains situational awareness of the maritime domain in cooperation with the Norwegian Coastal Administration (Kystverket). Below the NIS and FOH are situated the Cyber Defense Forces (CYFOR) with operational authority over satellite communication services, and the Navy, with responsibility for PNT-services (Eide, 2023, p. 22). An operational center for space operations was established in 2022 (Norwegian Ministry of Defense, 2024b).

The Arctic Surveillance Program (ASP) is an initiative established in 2023 that adopts a long-term and cooperative civilian-military approach to space capability development. The aim of the program is to gather key national stakeholders and increase the collective competency within the Norwegian space-related industrial base with the ambition to reach a complete national standalone capability to develop, launch and operate space assets vital for central national interests. The initiative is groundbreaking both in its scope and membership, with representation from the Norwegian Defence Research Establishment (FFI), the Armed Forces, Norwegian Space Center (NRS) and the Norwegian Coastal Authority at strategic and operational levels. ASP will develop a national system for space-based surveillance in the Arctic with a complete national value-chain for satellite capabilities (Hofoss et al., 2023, pp. 9–12).

The 2024 long term plan for the defense sector (LTP) confirms the current trend of emphasizing national space capabilities. The LTP states that the Armed Forces will be an “active participant in a comprehensive, national space initiative” with emphasis on close civil-military cooperation.[19] The independent launch capability provided by Andøya Spaceport is highlighted as an enabler for strategic autonomy. The ability to quickly replace satellites is an important contribution to NATO (Norwegian Ministry of Defense, 2024a, pp. 62–63). This capability plays a central role in Norway’s recent membership in the Combined Space Operations initiative (CSpO), a multilateral military initiative for the freedom of action in space (Norwegian Ministry of Defense, 2024b).

[16] See (Sundlisaeter, 2022) for an excellent elaboration on the history of these processes, and the entire Norwegian military space program.
[17] Original term: «Fagmyndighet»
[18] Original term: «Fagansvar»
[19] Original texst: «Forsvaret skal være en aktiv bidragsyter i en helhetlig, nasjonal satsing på det ytre rom» (Norwegian Ministry of Defense, 2024a, p. 62).

3 Understanding cyber operations

We continue with an elucidation of how to best understand cyber operations.[20] What is important to note from this section is the conceptualization for how an operation is conducted and what type of harm it can cause. These two aspects of cyber operations are important for the continued analysis. This section will also discuss the difference between cyber operations and adjacent terms of non-kinetic counterspace methods. But first, we begin with defining cyberspace and placing it within the structure of space infrastructure described above.

3.1 Defining the cyber dimension in space infrastructure

Cyberspace is defined as "encompass[ing] the hardware, software, data, and information systems, as well as people and social interaction within the networks."[21] The components of cyberspace are divided into three layers: physical, logical, and social. The physical layer refers to the hardware in the physical infrastructure underpinning the existence of the domain, including cables, servers, processors, and modems. [22] The logical layer, also called the software layer, includes the code, applications, computer systems, information, data packets and protocols transporting them. The social layer is often called the cyber-persona layer, and includes the human interactions enabled by the platforms and infrastructure (Van Puyvelde & Brantly, 2019).

When transferring this structure to space infrastructure, the result becomes as follows. The physical layer refers to all the hardware discussed in section two. The terrestrial cables for transport of satellite data, the antennae, command and control computer in the ground system, the space segment hardware, launch vehicles and supporting infrastructure, and the hardware of the user terminals and instruments. The logical layer points to the more explicit digital components in the systems. The code making up the software in the space segment command and data handling system, as well as the mission control software in the ground system for conduct of operations. Onboard processing in the space segment will also be included in this layer, as well as protocols and transport of data and the data itself. The social layer would in space systems refer to the personnel working with the development of the systems and the conduct of operations, as well as the users of the services.

Internet satellites have, as mentioned, a unique position in this context. On the one hand, they have their own in-house digital components, their command and data handling software and

[20] Many terms have been used to describe the exertion of power in or through cyberspace. Cyber *weapons* has been largely abandoned with the decline in popularity of the cyberwarfare concept (Zilincik & Duyvesteyn, 2023). A reason for this is the range of impacts a 'weapon' may have. Scholars have argued that 'capabilities' is a more fitting terms because "one cyber capability does not necessarily equate to another in the same way that one bullet is similar to other bullets" (Van Puyvelde & Brantly, 2019, p. 74). Cyber operations are now the most widely used term, figuring in the doctrines and policy discussions on the issue. See (Smeets, 2017; Kaminska et al., 2022; NATO Allied Joint Publications, 2020) for some examples.

[21] Definition provided by Jana Robinson (Robinson, 2016), referencing Martti Letho (Lehto, 2015, p. 6).

[22] See (Blount, 2019., Chapter 2) for an in-depth discussion on different approaches to defining cyberspace.

operating systems. On the other hand, their function as an internet satellite is comparable to internet cables, as part of the global connectivity infrastructure. Finally, timestamping services provided by GNSS-satellites are an enabling component in the synchronization of internet services. As such, it is a key enabler for the functioning of parts of the global logical layer.

As touched upon in the introduction of this report, the expanding digitalization of space infrastructure leads to larger components of space operations being transferred from the physical layer to the logical layer (Poirier, 2022). What the logical layer brings that is special is the option for remote access to data and processes in systems that are physically inaccessible. For example, software defined processes can be started, altered and stopped through commands in the logical layer, and the data stored in this layer can itself be of high value. What the transfer of parts of space operations to the logical layer creates is more possibilities for interference through offensive cyber operations leveraging the logical layer. The next sub-section will conceptualize this type of operations further.

3.2 Offensive cyber operations

Military cyber operations are operations undertaken by a nation-state military to achieve a strategic, operational, or tactical goal.[23] There are three types of operations within this frame. Aaron Brantly and Max Smeets (2020) describe them in the following way;

> *(...) (i) defensive cyber operations, those actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within a governments information systems and computer networks;*
>
> *(ii) cyber espionage operations, those actions taken through the use of computer networks to gather data from target or adversary information systems or network; and*
>
> *(iii) offensive cyber operations, those actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves, or in basic, operations designed to achieve tangible effects (...).* (Brantly & Smeets, 2020, pp. 3–4)

For the purpose of this report, the two latter types of operations will be grouped together under the term of offensive cyber operations because they are aimed at gaining entrance and/or achieving an effect in the systems of an opponent. Such offensive operations "employ capabilities aimed at achieving objectives in and through cyberspace" (Dinstein & Dahl, 2020, p. 19). *Capabilities* are understood as actions targeting the *CIA-triad*, referring to the confidentiality, integrity and availability of networks, their in-house data or data transfer (Van Puyvelde & Brantly, 2019, p. 57). Capabilities in this context are "[a] device, computer program, or technique, including any combination of software, firmware, or hardware, designed

[23] This definition is shared by many states (Brantly & Smeets, 2020). The US defines cyber operations as "the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace" (U.S. Joint Chiefs of Staff, 2017, n. GL 8).

to create an effect in or through cyberspace." (Computer Security Resource Center, n.d.) This includes different tactics for gaining access to information systems or to create an effect in the system. Examples are backdoors and different types of malware.[24] Capabilities can be centered on exploiting the human link through spear phishing campaigns.[25]

Breaching *confidentiality* means gaining access to proprietary data or confidential computer systems.[26] Harming the *integrity* of the system or data can be done through altering or deleting the data stored or transferred through it, or purposefully meddle with the functions conducted by the computer system. Examples may be creating a malfunction on a system operating virtual or physical processes, - such as online payments or production facilities. You can disrupt the *availability* of a system through denial-of-service attacks where the services provided by a system are made unavailable.

At a more granular level, offensive cyberoperations of this kind consist of different stages.[27] These are defined and structured in slightly different ways, but roughly consist of seven steps:

1. Reconnaissance: an actor gains knowledge of a system, its components and functions, and identifies which target suits a specific military objective. This includes the technical parts of a computer system but can also entail people that work with these systems.

2. Weaponization: the actor choses a target and pairs it with a chosen method or capability for obtaining the stated goal. This can be a chosen type of malware or other software-module that can create the wanted effect.[28]

3. Operation launch: the capability is delivered to the intended target.[29]

4. Exploitation: the vulnerability identified in stage one is exploited by using the method chosen in stage two and delivered in the suitable way in stage three. This can mean that the software module is engaged and executes its commands.[30]

[24] A backdoor attack is a way of evading the normal authentication procedures for gaining access to a system thorugh installing a clandestine entrypoint either through exploiting a vulnerability in the system or by using malware. Malware is an umbrella term referring to all computer programs or code that is used to harm computer systems. See (Belcic, 2023; Lutkevich, n.d.) for explainers.

[25] Spear phishing is a much-used method where one uses malicious emails that are tailored to the target with the aim of tricking them to share confidential information such as login details. Phishing emails are more general and are sent to larger groups of people with little or no personalization.

Password-spraying refers to attempting to gain access to a confidential computer system through

[26] All offensive cyber operations for espionage begin with point, before for example extracting data from a system.

[27] The chosen approach for this description leans on Brantly and Smeets (2020), whose understanding aligns with the Cyber Kill Chain-model of Lockheed Martin (Lockheed Martin, n.d.).

[28] The software capability needs to be tailored to the target system and can be developed inhouse or bought from actors developing them for profit. See Perlroth (Perlroth, 2021) for in depth description of this ecosystem. A software capability is constructed around a vulnerability in a computer system. Updating the software is a classical practice for closing the vulnerabilities.

[29] The delivery stage can be solely via computer networks as an email or as a man-in-the-middle attack, or potentially done physically via a USB-stick containing the software-module.

[30] If the vulnerability identified is a person with access the target computer systems, then this stage would be reached when the person, knowingly or unknowingly, enacts a function that gives the actor access to the target system.

5. Establishing a foothold in the system: this is most typically done through a backdoor that provides independent access to the system.

6. Remote manipulation: the actor manipulates the target system through the established backdoor.

7. Obtaining operational goal: the actor achieves the stated aim of the operation. This can be tampering with the information in the target system, such as a military system's targeting coordinates or the chemical composition of a water sanitation plant.[31] It can also be extraction of proprietary data or trigger an action in the target system that leads to a physical effect.[32]

A key aspect of an offensive cyber operation is that targeting one layer can cause an effect in another layer. Targeting the social layer (the people) through spear phishing can give access to the logical layer for installation of malware, corrupt or steal data. Inserting false data in a system or disrupting the availability of the systems (the logical layer) can erode the trust people have in the systems (social layer). Delivering a capability through a USB memory stick (physical layer), causing the system to malfunction (logical layer), and weaponize the human dependencies on the system for critical functions (social layer). This trait is important for the analysis in section four.

3.3 Cyber operations versus electronic warfare in space

A complicating factor when discussing cyber operations targeting space systems is the division between cyber operations and electronic warfare measures (EW).[33] Jamming is an EW measure where one interferes with the communication link by generating noise on the frequency. Spoofing is an EW measure where one injects a false signal on the frequency, and eavesdropping is listening in on another system's signals (Bingen et al., 2023, pp. 4–5). In the case of space systems, this division is complicated because the signal connecting the space segment to the ground and user segments is of a type that is traditionally within the realm of electronic warfare. Many technical scholars include jamming and spoofing in their treatment of cyber operations targeting space infrastructure (Fritz, 2013; Livingstone & Lewis, 2016; Manulis et al., 2021; Pavur & Martinovic, 2022; Thangavel et al., 2022). This is because the effect of EW attacks is the same as cyber operations targeting information systems' availability (jamming), integrity of information (signals injection) or confidentiality (eavesdropping). Some scholars define the up- and downlink signals to be part of the physical layer of the

[31] In 2020, Israel revealed a cyber operation allegedly of Iranian origin attempting to increase the amount of chlorine to damaging levels in a water sanitation plant. The operation appeared to be unsuccessful (White, 2020).

[32] These *effect*-operations are very resource intensive and are not possible for many computer systems. The promise of remotely delivered destructive operations with low attributability shaped the initial debates on the strategic value of cyberspace. The debates of deterrence and escalation in cyberspace spring from this point. See (Smeets & Soesanto, 2020; Stevens, 2012) for an overview of the deterrence literature in cyberspace. See (Lin, 2012), a seminal work in the cyber escalation literature.

[33] Some find the division so artificial that they prefer to group the two together in a CEMA term (cyber and electromagnetic activities).

infrastructure. Targeting the signal would therefore be similar to extracting or manipulating information carried within a fibreoptic cable.[34] In the context of this report, it is relevant to make a distinction between cyber operations and EW because the two groups carry qualitative differences that are relevant for how they are deployed, and consequently how to understand the risk they pose.

Several qualities of how offensive cyber operations function have been understood through cyber conflict research. One is that it is often challenging to attribute a cyber operation to a specific actor (Rid & Buchanan, 2015). Another is that the effect of cyber operations is often reversible[35] and a final is that there are challenges to both predict and verify a desired outcome of an operation before launch (Borghard & Lonergan, 2019). Electronic warfare means carry different qualities in terms of visibility, attributability, and verifiability of success. The target of a jamming or spoofing attack will be aware of what is happening, whilst most cyber operations need to not be discovered to be effective (Bingen et al., 2023).[36] Jamming and spoofing require a certain proximity, and need to be deployed at the exact time when the effect needs to occur. Cyber operations can be engaged in advance and be activated at will at a later time (Bingen et al., 2023). The range of possible results of a cyber operation is determined by the capabilities of the targeted system, while EW measures have a limited number of effects they can cause, making them less flexible. This report will follow a narrow understanding of cyber operations in space infrastructure, omitting attacks on the signal through EW measures. The signal is included as a communications link that may carry a cyber operation to the space or ground system, but not as an independent target of attack.

[34] See Daniel Moore (2022) for an excellent discussion in the shared and differentiating characteristics of cyber- and electronic operations. Theohari and Hoehn (2019) conduct a more practical and abbreviated analysis of the topic, also recommended.

[35] Cyber operations are ‘reversible’ in the sense that the systems targeted typically can be restored from backup systems after an attack. This presupposes that the owner of the system has access to it.

[36] See a comparison of different counterspace attack vectors, including EW and CO, in Bingen et al 2023 p. 6-7.

Norwegian cyber operations and the space sector

Norwegian doctrine for joint military operations defines cyber operations as; “military or strategic actions conducted within or through the cyber domain with the aim of ensuring freedom of action and target the enemy in order to achieve military or strategic aims.” (Norwegian Defense Staff, 2019, p. 125). Offensive cyber operations are under the purview of the Norwegian Intelligence Service (NIS) and are defined in doctrine as making use of; “active methods used to obtain and analyze information for intelligence purposes, or to harm, manipulate, disturb or influence personnel, material, information or activity, with the intention to create an effect at the opponent’s side”. The Norwegian definition groups cyber operations for effect and intelligence under the term offensive operations.

The Chief of the NIS holds the function as Cyber Commander with the mandate to coordinate all cyber operations within the Norwegian Armed Forces. This is to ensure that the defensive operations do not come into conflict with the offensive operations (Norwegian Defense Staff, 2019, p. 125, 129). Defensive cyber operations are under the responsibility of the Norwegian Cyber Defense Forces (CYFOR) and are under the command of the Chief of the Joint Headquarters (SJ FOH) (Norwegian Defense Staff, 2019, pp. 129).

Defensive cyber operations are defined in Norwegian doctrine as “efforts and activities initiated with the intent to secure and defend a military commander’s ability and opportunity to exercise military commands, control and communication by defending one’s own information systems” (Norwegian Defense Staff, 2019, p. 126). The efforts in defensive cyber operations refer to defending against or stopping incoming cyber operations from an adversary, and to reduce damage from incoming cyber operations and handle its consequences. CYFOR holds the responsibility for conducting defensive cyber operations as well as being the operational authority for military satellite communication (Norwegian Defense Staff, 2019, pp. 125–126).

The Norwegian government has emphasized a need for strengthening the resilience of public services and functions considered critical for Norwegian society, such as health services, power- and food supply, the freedom of national political institutions and satellite services (The Norwegian Directorate for Civil Protection (DBS), 2016, p. 9). The Norwegian National Security Authority (NSM) is a cross-sectorial agency under the Justice Department that is charged with supervisory authority over the cyber security in the space industry. NSM’s Cyber Security Center is the national point of contact for the security of ground-based space infrastructure on Norwegian territory (Norwegian Ministry of Trade, Industry and Fisheries, 2019, p. 52).

4 Cyber operations targeting space infrastructure

This section will apply the conceptualization of offensive cyber operations presented in the previous section onto components of space infrastructure. There are few known empirical cases of cyber operations targeting space infrastructure. The following analysis will build on some empirical cases, but mostly lean on theoretical technical research on possibilities for offensive cyber operations.[37] The two sub-sections follow different structures, but both incorporate the same factors of; *how* an actor can gain access and *what* effect it can cause with an offensive cyber operation.

As described in section three of this report, a key characteristic of offensive cyber operations is that an action in one layer can cause an effect in a different layer. As illustrated through the discussion, obtaining access is only a means to an end, which put simply is to either monitor, extract, manipulate or destroy the data stored in or flowing through a system, or tamper with the processes the system controls. There is therefore an important division between the segment where an intruder *gains access*, and where the *effect* of the operation is happening. In the following discussion, this division will be highlighted.

The following sub- sections are structured as follows: The analysis begins with discussing the possibility for offensive cyber operations targeting the ground segment. The two key components here are the ground station and the infrastructure for obtaining Space Domain Awareness. From there on, operations targeting the space segment are analyzed in two steps. The first step focuses on the cyber vulnerabilities highlighted in the literature to show how an actor can gain access to the systems. I then describe examples of effect obtained through offensive cyber operations. This part leans primarily on experimental analyses showing proof of concept.

4.1 The ground segment

The ground-based components of the space infrastructure are the most exposed for offensive cyber operations because of the sheer number of entry points. In an official audit published in 2014, the US Department of Commerce’s Office of the Inspector General found more than 9000 high-risk issues in the ground infrastructure of the Joint Polar Satellite System of the National Oceanic and Atmospheric Administration (NOAA) (US Department of Commerce Office of the Inspector General, 2014). A cyber operation may obtain access to the ground segment through all three layers in this segment, via physical access to the infrastructure, through the logical layer via digital intrusion, and by exploiting the human link to gain access. An operation may be aimed at obtaining an effect in the ground segment itself, or as a jumping point to creating an effect in the space segment.

[37] The majority of empirical evidence of targeting of space infrastructure has been on the signal. See the appendix published with (Pavur & Martinovic, 2022) for an overview.

4.1.1 The ground station

Ground stations are often ill-secured from both physical and digital intrusion attempts. Air-gapping is a much-used technique for limiting the vulnerability to digital intrusions through the logical layer. Air-gapping is done by creating a separate computer system isolated from the internet. This is typically secured through procedures for limiting the possibility of transferring data or files between the external, internet-connected computer system and the closed internal system. This makes gaining unauthorized access much more challenging. Air-gapping is standard for critical infrastructure systems, but not a widely deployed practice among space actors (Falco, 2018; Graczyk et al., 2021). The data flowing from space systems is often meant for public consumption, which makes it unpractical to have them completely air-gapped (Harrison et al., 2021).[38] Ground stations may be of varying sizes and sophistication. Those of the simpler variety often have weak physical protections because they are remotely located (Pavur & Martinovic, 2022, p. 12). This makes intrusion through physical access easy with unsophisticated methods. The ground station computers are also often easy to identify using standard IoT-search engines, adding to the risk of them being identified and targeted (Santamarta, 2014, 2018).

When a malevolent actor has gained access to the ground station, mission control software may be compromised and remotely accessed to send faulty commands to the space segment (Graczyk et al., 2021). The people operating the ground station can be tricked into providing access to the computer systems and the attacker may then be able to install a backdoor to remotely operate the system or install malware that makes the system unavailable (Pavur & Martinovic, 2022).[39] If the satellite collects data from orbit, the collected data received from the space segment can be corrupted upon arrival to the ground station. If the integrity breach of the data goes undetected there may be cascading errors in the systems dependent on the information (Graczyk et al., 2021; Pavur & Martinovic, 2022).

The ground station is the critical single point of failure for a space system. If it loses contact with the space segment it may not be able to reconnect, and the satellite and the capabilities it provides are lost. Space assets do need to adjust their orbits from time to time, either due to mission requirements or because of collision hazards with debris or other space assets. Losing access to the mission control software temporarily through a cyber operation can be critical if there is an urgent need to maneuver the satellite (Sanchez & Zatti, 2020, p. 254). Issuing ingenuine commands from a compromised ground station can also cause the satellite to alter its orbit, disrupting its own mission or potentially collide with another satellite (Sanchez & Zatti, 2020, p. 254).

[38] Some operators have made the conscious choice to airgap only the system for communication with the space segment, while having internet connectivity to on the rest of the ground stations systems. However, physical proximity of the systems as well as possible careless management of the systems can compromise the air gapped system (Fritz, 2013). A case study from 2013 of identified vulnerabilities at NASA ground stations some years prior where weak risk management of internet connectivity on ground station systems was central (Fritz, 2013, pp. 30–34).
[39] Examples include wipers and ransomware that encrypt the content of your computer system, and either simply delete the encryption key, or attempt to extract a ransom for providing it to the owners of the system, respectively.

There are empirical cases of actors losing control over their space segments to an adversary due to intrusions in the ground station. In 2007 and 2008, NASA lost control over two satellites for several minutes. Initially, the events were reported as signals jamming, but were later linked to Chinese actors compromising the ground stations and their command and control function (Arthur, 2011; Pavur & Martinovic, 2022). There have been similar accusations from NASA in the following years, all connected to Chinese actors (Flaherty et al., 2014; Loughran, 2018). One such event was in 2014 when National Oceanic and Atmospheric Administration (NOAA) revealed that a nation state believed to be China had gained access to the software for command and control at the ground station and the system for uplink commands. The attackers managed to force the system to go offline, resulting in NOAA not publishing its satellite imagery online for over a week (Bichler, 2015).[40]

A state affiliated hacker group was revealed in 2018 to have compromised the space mission networks of the Jet Propulsion Lab (JPL).[41] Sources state that the access to the system may have been maintained for almost a year prior to being exposed. The access provided the ability to disrupt critical communication systems but were not reported to have been executed. The intruders did nevertheless manage to exfiltrate sensitive export regulated information from the system (NASA Office of Inspector General, 2019). A cyber operation the following year leveraging a zero-day vulnerability[42] gave the attackers access to the JPL specialized satellite operation software (NASA Office of Inspector General, 2019). This operation was revealed and halted before the attackers could use the access to interfere with operations.

4.1.2 The Space Surveillance Network (SSN)

As described in section two, most space actors rely on data from the Space Surveillance Network (SSN) to maintain an adequate space domain awareness. SSN-data is collected from a globally dispersed infrastructure and transported from its different locations to be processed and collated into a complete image of the orbiting objects and their trajectories. This final *space picture* is then utilized by many actors, private, public and military alike. The data collected and processed within this network may be subject to intrusion and compromise. Two ways this may occur is during classification of the registered objects in orbit and in the data on their trajectory prognosis. In the case of the former; a malevolent actor could manipulate the signature data of an registered object, tricking the system to classify an intelligence gathering satellite as space debris, alternatively to shield it from being registered at all (Pavur & Martinovic, 2021).[43] This makes it possible to covertly get close enough to a satellite to eavesdrop on their signal, and possibly inspect or interfere with the system without its operators being aware (Pavur &

[40] (Bichler, 2015) as referenced in (Thummala, 2023).

[41] The Jet Propulsion Lab is a research and development organization under NASA , which is operated by California Institute of Technology (CALTech).

[42] A zero-day is a type of vulnerability in a computer system that is open to be exploited without extensive preparation.

[43] This concept has been proved through simulations conducted on genuine SSN-data. See (Pavur & Martinovic, 2021)for details.

Martinovic, 2021). Such operations are called rendezvous and proximity operations (RPO) and have occurred on several occasions.[44]

Data from the SSN-network may also be manipulated on the orbit trajectory-function. If one's asset is on a collision course with another orbiting object, satellite operators receive a warning that they must alter the orbit of their space asset. Simulations on genuine SSN data have demonstrated how a malevolent actor who has gained access to the infrastructure through the logical layer may with some ease inject false data in the SSN-system (Pavur & Martinovic, 2019). The satellite operator would then receive a warning about their system being on collision course with another satellite or piece of debris, prompting them to alter the trajectory of their satellite. This could disrupt the operation, or if conducted extensively, cause the satellite to waste its limited fuel supply. In a worst-case scenario, the incorrect picture the operators then have of the situation may cause them to maneuver their asset into a space they believe to be open, but that in truth results in them colliding with another satellite (Pavur & Martinovic, 2019). This would be a case of achieving an anti-satellite capability through an offensive cyber operation.

4.2 The space segment

A space segment in orbit is for all practical purposes physically inaccessible. If a malevolent actor wishes to access the system via the physical layer, this must be done in the development phase before it is launched. Access via the logical layer can also be done before launch, where an actor prepositions itself in the software of the satellite, for example in the command and data handling component, or in the software connected to the functioning of the systems payload (Graczyk et al., 2021, pp. 10–13). Access through the logical layer after launch would have to be done through the communications link of the system. A compromised ground station may, as mentioned, issue faulty commands that can ultimately breach all the components in the CIA-triad of the space segment. A malevolent actor may access confidential information collected by the satellite and the integrity of the data could be harmed by interfering with the onboard data processing procedures. The services provided by the satellite may be made unavailable to the users that depend on them (Graczyk et al., 2021; Theohary & Hoehn, 2019). One example is the command and data-handling component of the satellite being manipulated to move the satellite out of orbit or shut off critical functions. In the case of the satellite having a software-defined radio, an alteration in the system's software can transform a radio from a receiver to a transmitter, disrupting the ground station's communication with the satellite (Theohary & Hoehn, 2019).

Access through the social layer mirrors the two avenues for access discussed for the logical layer before launch and after via the communications link to the ground station. People with

[44] Rendez-vous and proximity operations are operations where a satellite move close to another satellite on orbit, and potentially intercepts signals, inspect the hardware, and in extremis, interferes with the system. A well-known example is the Russian Luch satellite what has been registered as maneuvering close to US communication satellites on several occasions, also in time periods that coincide with the build-up to and early months of the invation of Ukraine in 2022 (Bingen et al., 2023, p. 17).

access to the computer systems involved in system development or operation may be tricked to give a malevolent actor access to the relevant computer system. The intruder would then introduce a malicious software module. Access to the ground station could allow the actor to issue updates to the satellite's software that contain malicious modules. As touched upon, many ground stations do not have their command and control systems separated from the internet. Unsophisticated methods such as brute force entry attempts[45] or phishing email could grant a malevolent actor access to the systems that issue commands to the space assets.

4.2.1 Vulnerabilities putting the space segment at risk

The literature points to several practices common in the space industry today that increase the vulnerability of the space segment to offensive cyber operations. One is the openness of the communication link to the space segment. Many actors have few procedures in place to ensure confidentiality and integrity of the data flowing to and from the space segment, such as authentication procedures (Graczyk et al., 2021; Thummala, 2023). Satellite software typically follows an "open trust" model, where a ground station is trusted by all devices aboard the space platform (Pavur & Martinovic, 2022, pp. 11–12). Authentication procedures typically protect against other entities gaining unauthorized access to computer systems. Lack of such procedures in the satellite's communication with its ground station makes it easier for malevolent actors to trick the space segment to provide access to its systems and accept disingenuous commands. Encrypting the signal secures it from confidentiality breaches, but since the link capacity is a limited resource, using some of this for encryption is not always prioritized (Pavur & Martinovic, 2022, p. 8). For commercial actors, for example, encryption is not typically standard (Fritz, 2013, pp. 7–8; Harrison et al., 2021, p. 16; Pavur & Martinovic, 2022, p. 8). If the communication link is encrypted, the key for decrypting it is held by the ground station and the space segment. In the case of a malevolent actor managing to replace the encryption key and take control of the satellite, they may operate the system for their own purposes, or instruct it to go into survival mode. They could also manipulate the sensors to turn directly into the sun and be incapacitated (Graczyk et al., 2021, p. 15) [46]

As pointed to in section three, identifying software vulnerabilities is a starting point for many types of offensive cyber operations. They may be used to gain access to a system or create an opening for causing a tangible effect. Software vulnerabilities are a common occurrence in all software and regular patching is issued through software updates to close them. However, researchers have pointed out that procedures for patching software in satellite systems are not typically strong (Falco, 2018). Overflight time and link capacity are two reasons for this. If the satellite in question is placed in LEO, the overflight time is 10-15 minutes and the capacity on the link is limited. This often leads to the satellite operators skipping updating cycles, leading to unpatched vulnerabilities in the systems (Falco, 2018).[47] Software updates also require system

[45] Brute force attacks are also called password spraying attacks and refers to a hacking method where one uses trial and error to crack passwords or encryption keys. Attackers can use a computer program to at speed guess login usernames and passwords (Fortinet, 2023).

[46] Similar types of threats are pointed to by Harrison et al (2021) and Bingen et al (2023).

[47] Lack of updating procedures has been the reason for many malware attacks, most notably the Wannacry ransomware attack which incapacitated the UK National Health Services among others in 2017 (Collier, 2017).

downtime, making the services unavailable for the time it takes to update. Gregory Falco described the situation as follows:

> *"Not dissimilar to industrial control systems, space assets are built to last and because they are functional in the field for such long periods and are mission critical, system downtime is not an option. This makes space assets difficult if not impossible to patch for security flaws that are discovered."* (Falco, 2018, p. 4)

The use of commercial off the shelf (COTS) systems contributes to keeping the costs of gaining access to space down. However, important security concerns are tied to the use of COTS in space segments (Falco, 2018; Graczyk et al., 2021; Manulis et al., 2021). One is that commercial systems are dependent on regular software patching to stay secure and effective. As touched upon above, software updates are challenging and often not prioritized by satellite operators. A second security concern is that since the COTS are commercially available, a malevolent actor can gain intimate knowledge about the system and its software, learning more about how to potentially alter it for offensive purposes (Falco, 2018; Graczyk et al., 2021; Manulis et al., 2021). The traditional 'security through obscurity' concept held that information about how satellites function and how they could be tampered with was so challenging to obtain that it in itself was an adequate security measure. This stance is no longer valid due to the widespread use of COTS and general openness around satellite operations and technology stemming from the commercialization of the industry.

The software in COTS systems is often *open source*, meaning that anyone can inspect and alter the code in the software. Some authors hold that the open source nature to COTS software means that malevolent actors can contribute to the code themselves, inserting backdoors to be exploited on a later time (Falco, 2018).[48] The US agency Cybersecurity and Infrastructure Security Agency (CISA) has pointed out that COTS software programs function as 'black boxes' for their clients (Cybersecurity and Infrastructure Security Agency (CISA), 2022). This means that a software purchaser has little ability to exercise any real control of the inner workings of the software of a system.

The use of COTS increases the risk of being targeted with offensive cyber operations in yet another way. Offensive cyber operations for physical effect, where one makes the physical components of a system malfunction through altering the software of the system, are very challenging to conduct successfully. A main reason for this is the limited knowledge one typically has about the systems of an opponent. The opponent's system will typically have securing mechanisms that may alter the course of the intended cyber operation. To be certain that the operation has the desired effect, one needs to test different approaches on the actual target system. This testing is easier to conduct when one can have access to the system itself for extended periods of time before launching it into orbit (Falco, 2018; Graczyk et al., 2021; Manulis et al., 2021).

[48] This claim is disputed as many would argue that open source code tends to be more secure because anyone can edit it, and thus reveal any attempts for malevolent interference. See (Meyers & Kazil, 2023) for a discussion.

The commercial space industry has qualities that contribute to the vulnerability of both the ground and space segments. The complex structure of contributors to production, maintenance and ownership of the infrastructure entails that the responsibility for cyber security is spread over several entities within several specialized fields making it challenging to manage risks (Falco, 2018, pp. 4–5).

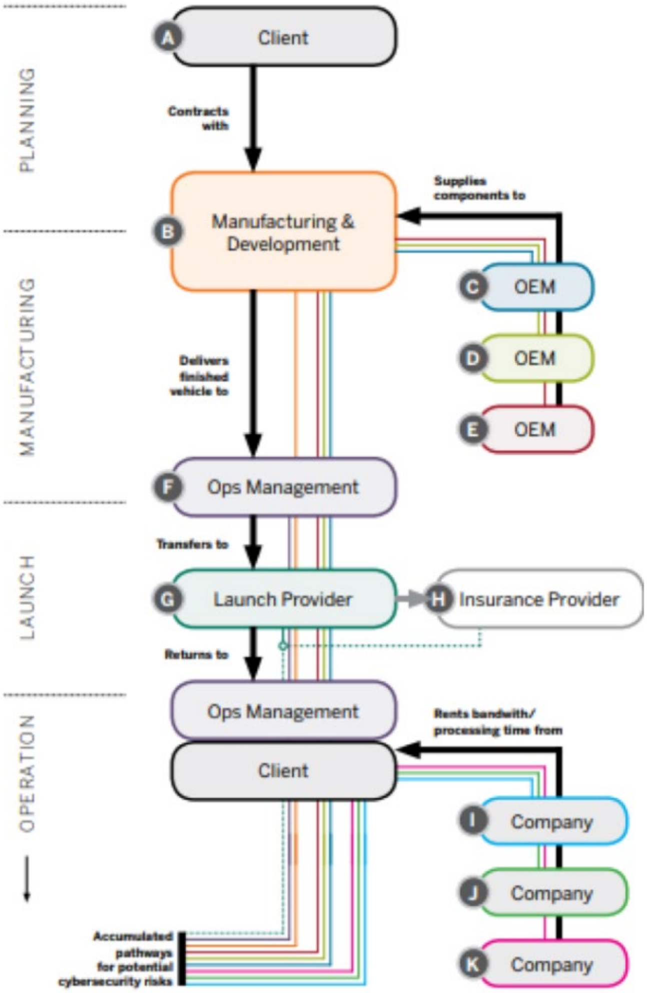


Figure 5.1 Example of cyber security responsibility landscape across a supply chain. OEMs in point C,D and E are companies providing components of the satellite to the manufacturer (B) (Falco, 2018)

Figure 5.1 shows an example of the many actors involved in the supply chain of a satellite project from planning through to operation. The OEMs in point C, D and E illustrate companies providing components of the satellite to the manufacturer. According to research on the issue, cyber security requirements are not necessarily included in the authorization procedures of vendors that are to deliver components to space systems utilized by states (Falco, 2018, p. 3). The number of actors involved in operations at different stages also makes access control[49] difficult to manage and increases the chance of unsophisticated phishing attacks compromising the system through the social layer (Falco, 2018). This makes the systems vulnerable to supply chain attacks, where a malevolent actor gains access to a high value target through compromising one of the smaller components in the supply chain.[50]

[49] Access control refers to limiting the number of people with access to certain computer systems or data as a means to minimize the vulnerability of the systems or data being compromised. The control can be either physical, referring to physical spaces, or logical, referring to computer systems (Lutkevich, 2022).

[50] The 2020 Solar Winds hack is a text-book example of a supply chain attack, where a state affiliated actors managed to install a back door in the systems of several thousand customers of the company SolarWinds' Orion software, thereby gaining access to the networks and data. The customers included US government agencies, such as the Department of Homeland Security and the State Department, and commercial companies like Microsoft, Intel and Deloitte (Oladimeji & Kerner, 2023)

4.2.2 Examples of effects in the space segment

Empirical cases of offensive cyber operations targeting the space segment are rare, but scholars have conducted simulations and experimental technical analyses that explore technical possibilities for the space segment falling victim to such operations. There are for example yearly 'Hack-a-sat' competitions initiated by the US Space Force that test how different attack modi via cyberspace can affect a satellite in orbit. These are typically conducted via online simulations, but in 2023 they used a satellite put in orbit for this purpose (McKay, 2023).[51] Other companies and organizations have online simulation where the public may simulate satellite functions and different ways of reinstating control after an offensive cyber operation.[52] Some effects obtained through such activities have been making the space segment enter into survival mode, and tricking it to report a false location to its ground station (McKay, 2023).

In a recent study, researchers simulated a concept where a SpaceX commercial launch vehicle was targeted by a customer (Pavur et al., 2021). SpaceX has regulations for what capabilities a satellite may carry on board its space rocket. The structure, called a "launch bus", often carries over a hundred satellites into LEO on its launch vehicle. The researchers revealed that the control mechanisms for upholding these were weak and often dependent on self-reported compliance. By combining insight from open-source requirements for the hardware and software of the satellite, as well as software criticality indexes and control mechanisms for ensuring compliance, the researchers demonstrated the level of difficulty of equipping the satellite with a capability to carry a malicious payload (Pavur et al., 2021). The result revealed that it was quite possible for a malevolent actor to be successful.[53] The Falcon Heavy launch vehicle Space X uses for such operations has a fully autonomous landing phase, and therefore has automated security measures in place in case of system malfunction. The authors' experiment demonstrates a possibility of interfering with the launch system's navigation, tricking it to believe it is off course, triggering an automated security response like a self-destruct effect (Pavur et al., 2021). Revealing the origins of such an operation would be particularly challenging since the systems on which one could find forensic evidence of the cyber capability would be in orbit and physically inaccessible.

Another similar example focuses on the possibility of satellite constellations spreading malicious software from one compromised satellite to the rest in the network. Satellite constellations have communications links not just to their ground segments, but also to the other satellites in their constellation. These are called crosslinks, and the constellation functions as a relay-network with each satellite being a node in the system (Thummala, 2023, p. 18). The internet satellites in LEO are of this category and use the crosslinks to adjust orbits to changing mission requirements, and to transfer commands from the ground station to all nodes in the system (Thummala, 2023). These crosslinks between satellites can transfer malicious software

[51] https://hackasat.com/. Details of the conduct of the 2023 operations can be found in the teams' technical reports via (Mhackeroni, 2023)

[52] Examples include the CubeSat Simulator (https://cubesatsim.org/) built by the Radio Amateur Satellite Corporation.

[53] See table in (Pavur et al., 2021, p.160) for details on the distinction between results for malicious *insiders* and *outsiders*.

that may trigger a physical effect in the receiving system. This has been proven through a limited experiment deploying a type of malware known as a computer worm (Thummala, 2023). Additionally, the inter-satellite link can be exploited to trick the satellite to think that it has already reached its determined placement in orbit or to exit its assigned orbit (Falco, 2020). This type of manipulation may be particularly relevant for internet satellites since they currently make up the largest constellations in orbit.[54]

4.3 Categorization and summary

The analysis in this report has shown how the ground and space segments in space infrastructure may be exploited through offensive cyber operations. This sub-section will summarize the above analysis through highlighting the effects that may be obtained through offensive cyber operations, as well as outlining two main groups of cyber security vulnerabilities revealed through the analysis.

4.3.1 Summary of effects

Space systems provide services that can be divided into whether the added value of the system comes from collecting data from orbit, or whether they provide a relay or positioning and synchronization service. PNT, communication and internet satellites are examples of fall within the latter category, and earth observation satellites in the former. Both groups will have varying options for contingency should they be disrupted or degraded. The analysis conducted in this report has exemplified how offensive cyber operations could corrupt data collected in orbit, make any type of satellite service unavailable, or tamper with the satellites onboard processes. All such events may create cascading effects but the severity of these will depend on whether the services are time sensitive or not.

An offensive cyber operation can breach the integrity of the data collected from orbit to either degrade or destroy it. This data can also be illegally accessed or stolen, meaning a breach of confidentiality. Disrupting the access to data streams or services provided by the system can be done through both the space segment and the ground station, which would critically impact all functions dependent on the services that do not possess back-up options. Manipulating the satellites placement can be done through tricking the satellite to report a false location to the ground station. Access to the systems could be disrupted temporarily and later reinstated. However, if this happens at a critical time such as when the space segment needs to maneuver to avoid debris or to achieve mission requirements, it may have more severe consequences.

A satellite operator can permanently lose control over its space asset to a malevolent actor. This may be achieved by replacing the encryption key and take control of the satellite or trick it to go into survival mode. A threat actor could also destroy the satellites sensors by turning them

[54] To date, there is only really one example of internet satellites playing a role in a cyber operation. The Russian affiliated cyber threat group Turla was revealed in 2015 to have used an internet satellite connection to exfiltrate data stolen from a compromised computer system. The method left few traces, but researchers found forensic traces indicating that this method could have been used as far back as 2007 ("Satellite Turla," 2015).

directly toward the sun or move the satellite out of the orbit needed for its mission. The navigation of a launch vehicle may be interfered with through a compromised on board satellite, potentially triggering automated security responses in the vehicle.

Data required to achieve Space Domain Awareness can be manipulated to trick the satellite operators to maneuver the satellite out of its position, disrupting conduct of operations or possibly crashing with another asset. Manipulated classification data can also facilitate an adversary's satellite to conduct rendezvous and proximity operations undetected and obtaining an intelligence advantage.

4.3.2 Categorization of vulnerabilities

This report has used the vulnerabilities put forth in the space-cyber literature to describe the potential for offensive cyber operations from a motivated actor. Two groups of vulnerabilities have been identified through the analysis. The first are the vulnerabilities following from the practices and culture in the contemporary space industry. The openness of information about space technology and software, and processes and procedures are important facilitators for innovation, cost saving measures, and for the access of small actors into the industry. The use of COTS and commercial software are effective for many actors looking to the commercial market for inexpensive components for their space programs and entail supply chains that are open and competitive. Transparency is necessary to ensure fruitful and democratized competition, but it also creates an opening for states wishing to gain access to information about potential targets and to plan operations.

The second group of vulnerabilities stem from the lack of implementation of well-known best practice for ensuring adequate cyber security. The following are all low-hanging fruits of risk mitigation practices within the field of cyber security: authentication procedures, updating software, encryption of data and the signal, air-gapping of critical systems like a command-and-control computer at a ground station, ensuring access control for persons involved in the development of space infrastructure and conduct of space operations, and finally, physical securing of high value systems.

The reasoning for these not being implemented is twofold. Firstly, there are impracticalities stemming from the physical qualities of space technology and infrastructure. The capacity on the signal to the space segment is limited and the overflight time is short, which inhibits software updates and encryption. Authentication procedures would also demand using this limited resource. The fact that satellites often have an open-trust model is to limit the risk of accidentally losing contact with the segment, which has happened on several occasions (Marples, 2022). Making security updates to the hardware of the space segment remains impossible, at least for the time being. Secondly, the New Space industry is still in its youth and is yet to establish a security culture incorporating an understanding of the cyber threat landscape. The limited attention allotted to cyber security responsibilities and risk in the supply chain of the space industry is a testament to this. As are the lacking procedures for access control, air-gapping and physical securing of critical systems. Lack of empirical cases understandably has an important role in why these issues have not been a priority. We are currently in the first wave of the New Space trend and the momentum is focused on getting off the ground and into the domain. Since orbits are reserved on a first-come first serve basis, actors need to act fast.

5 Conclusion and recommendations

The research question guiding this report was “how does the space-cyberspace nexus influence the risk of offensive cyberoperations targeting space infrastructure?” The analysis has answered the research question by showcasing the potential avenues for gaining access to and creating effects in key components in space infrastructure. Risk was understood as containing two components; *probability* and *impact*. The analysis has exemplified how offensive cyber operations have the ability to corrupt the data from, access to or processes conducted by the space segment. The impact may be wide-ranging, from losing contact with the space segment, incapacitating the command-and-control software, intercepting confidential data or altering or destroying data from the satellite. A motivated actor may gain an intelligence advantage through rendezvous and proximity operations from manipulating the object classification data within the SSN-system. The space segment may impact with other satellites if the orbit prognosis data is manipulated. All for these events can cause cascading effects in the operations, systems and services depending on space services.

Assessing the probability was done though analyzing how offensive cyber operations *could* be deployed to space infrastructure. This approach focused on the technical openings and relative difficulty of such operations by pointing to vulnerabilities in the ground and space segments highlighted through the literature. The analysis indicates that the bar for exploiting space systems may be lower than we would prefer. Vulnerable supply chains, lack of prioritization of cyber security, and the opening to familiarize oneself with the commercially available space technology for planning operations point in this direction. The openness of the space industry is a key enabling factor ensuring the democratized access to the technology and domain. It is, however, also a factor that can be exploited by motivated actors. This translates to an increased probability for motivated actors using this option. The digitalization of the space systems does provide an opening for gaining access to data and processes conducted by the space systems but it is the lack of attention to cyber security principles in the industry ecosystem that seem to fail in mitigating the risks.

There are few empirical cases of offensive cyber operations targeting space infrastructure, and this may be a contributing factor to the low attention to cyber security in the ecosystem. However, the lack of cases is not necessarily due to the technical possibilities but because states have not yet found it beneficial to leverage this tool for offensive purposes. There are different perspectives on why states refrain from using this tool. The fear of retaliations may have contributed to a *mutual deterrent effect* between states where the knowledge of opponents’ ability to respond symmetrically keeps states from using it. Some scholars are pointing to cross-domain deterrence as the reason, where military might in other domains create a deterrent effect in cyberspace or outer space (Bahney et al., 2019; Schneider, 2019). It may also be the fact that the lack of open direct conflict between states with the most advanced offensive space- and cyber capabilities is the main reason for the few empirical cases. If they are used more covertly in inter-state competition, they may be kept from the public eye because of confidentiality requirements. Nevertheless, the technical possibilities for exploitation appear as the most prudent starting point for a comprehensive understanding of the risk of this class of threats.

Looking forward, the exponential growth of systems in orbit and expansion of the New Space industry signifies more services and actors using and developing space infrastructure. There is much technology development in this field that is currently in its infancy but aims at offering more and new types of space services. By extension, dependency on space infrastructure may become more widespread in the future, but the increase in space actors may also create redundancy and open for quickly reinstating access to services. Technological developments for on-orbit servicing are underway, and may also aid in repairing and updating hard- and firmware of satellites, which would mitigate some vulnerabilities in the space segment.

5.1 Recommendations and further research

The brief description of cyber operations targeting space infrastructure shows a span in consequences of these kinds of operations. The research presented in this report leads to several recommended courses of action that would aid in strengthening the security and resilience of space infrastructure against this class of threats:

- **Promoting comprehensive risk assessments;** states and commercial companies in the space sector should be cognizant that this is an avenue for attack and seek robust risk assessments from communities with comprehensive competency in the landscape of cyber threats. Cyberspace is crowded with a mix of non-state, state, semi-state, and proxy actors. The different actors should be included in a risk assessment to create a holistic understanding of the span of threats in the domain. A risk assessment should consider the technological possibilities for exploitation, and not build the risk perception exclusively on the empirical record in the domain.

- **Enhanced cyber security procedures** through implementing best practices of cyber security standards in the space sector. Examples of this would be to ensure prioritization of encryption on signal and software updates on the space segment, air-gap and physically secure critical systems in the ground segment, and enact proper access control through the supply chain.

- **Promoting a robust security culture across the space industry;** including advancing an understanding of the vulnerabilities stemming from the nature of the New Space industry, particularly related to its openness and use of COTS, and implement the necessary risk reducing measures in national space programs.

- **Improved supply chain security** within the space industry with emphasis clear cyber security responsibilities.

- **Preparedness through contingency planning and scenario-based implication analysis**. Actors dependent on space services for critical civilian and military functions should engage in scenario-based implications simulations and exercises with the aim of understanding the cascading effects and construct contingency plans. The options for contingency through international support should be considered when deciding on the adequate level of security afforded to the system.

5.1.1 Recommendations for Norway

Norway as a space actor is rapidly developing its satellite fleet and space industry. Some of the recommendations presented are already in development such as the work to ensure a complete national standalone capability to develop, launch and operate space assets vital for central national interests. Nevertheless, the research conducted through this report has highlighted several points relevant for the Norwegian space sector.

- **Norway should seek robust threat assessment** on cyber threats against the space sector and **ensure comprehensive dissemination across the public and private actors.** Norway's strategic focus on the High North and satellite capability development in the Arctic makes it particularly important to obtain and share a comprehensive understanding of all avenues of hostile action against this type of strategic infrastructure. The Arctic Surveillance Program forum may be an appropriate arena for sharing perspectives on the threat landscape.

- **Include offensive cyber operations against space infrastructure in scenario based contingency planning** to better understand the shape and extension of cascading effects. This should include different types of cyber operations on different types of both national capabilities and allied infrastructure that impacts Norway trough international cooperation. This can take the form of both military exercises and simulated analyses and should be used to understand implication in a strict military setting and in a Total Defense frame including implications for critical societal functions. The analyses should be used to develop the national infrastructure to become more resilient.

- **Norway should be cognizant of the typical vulnerabilities** present in the New Space-industry and **take steps to mitigate these**. This may be particularly relevant on the use of COTS.

- Include a comprehensive **understanding of the risk from offensive cyber operations within the competency promotion functions in the Arctic Surveillance Program**.

The technological possibilities for exploitation should be the starting point for the risk perception, and not lean solely in the empirical record of activity in the domain.

- **Ensure hardening of the systems connected to the development of the independent launch capability at Andøya**. This is because the installation represents a capability of strategic importance.

Further research should explore more in depth the degree to which different New Space actors are incorporating the best practices of cyber security in their development and conduct of space operations. Examining the supply chains of selected projects, and how cyber security risk treated across the many actors and responsibilities would aid in understanding the scope of the problem. Finally, conducting a scenario-based analysis on the implications of low-, medium, and high-severity offensive cyber operations targeting space missions would aid in the understanding of cascading effects of these tools.

The digitalization of space systems is a trend that develops in parallel with the increase of actors in the space domain and the lack of rules and regulations for capabilities and activities. Offensive cyber operations are a daily occurrence through the terrestrial cyberspace. We have yet to understand what the elevation of the militarized cyberspace into orbit entails for security and strategy. Although we have accumulated some experience in understanding the scale and scope of offensive cyber operations, we have less experience with operations of a certain magnitude between states, and even less when it comes to cyber operations targeting space infrastructure. This creates a need to expand our understanding of this class of threats through further research.

References

Arthur, C. (2011, October 27). Chinese hackers suspected of interfering with US satellites. *The Guardian*. https://www.theguardian.com/technology/2011/oct/27/chinese-hacking-us-satellites-suspected (accessed 15.10.2023)

Bahney, B. W., Pearl, J., & Markey, M. (2019). Antisatellite Weapons and the Growing Instability of Deterrence. In E. Gartzke & J. R. Lindsay (Eds.), *Cross-Domain Deterrence: Strategy in an Era of Complexity*. Oxford University Press. https://doi.org/10.1093/oso/9780190908645.003.0006

Belcic, I. (2023, August 25). What Is Malware and How to Protect Against Malware Attacks? *What Is Malware and How to Protect Against Malware Attacks?* https://www.avast.com/c-malware (accessed 15.10.2023)

Bichler, S. F. (2015). *Mitigating Cyber Security Risk in Satellite Ground Systems* Masters thesis at Air Command and Staff College, Alabama.

Bingen, K. A., Johnson, K., Young, M., & Raymond, J. (2023). *Space Threat Assessment 2023*. Center for Strategic and International Studies (CSIS). https://www.csis.org/analysis/space-threat-assessment-2023 (accessed 18.04.2024)

Birkeland, R. (2022). Satellitt. *Store norske leksikon,* https://snl.no/satellitt (accessed 21.08.24)

Bjerke, P., & Olsen, R. (2008). *En introduksjon til satellitter* (08–01751). Kjeller: Norwegian Defence Research Establishment (FFI). https://ffi-publikasjoner.archive.knowledgearc.net/bitstream/handle/20.500.12242/2177/08-01751.pdf

Blount, P. J. (2019). *Reprogramming the World: Cyberspace and the Geography of Global Order*. E-International Relations Publishing ISBN: 978-1-910814-52-9

Blount, P. J. (2017). Satellites Are Just Things on the Internet of Things. *Air & Space Law*, *42*(3), 273–294.

Borghard, E. D., & Lonergan, S. W. (2019). Cyber Operations as Imperfect Tools of Escalation. *Strategic Studies Quarterly*, *13*(3), 122–145.

Boschetti, N., Gordon, N., & Falco, G. (2022, October 24). *Space Cybersecurity Lessons Learned from The ViaSat Cyberattack*.

Brantly, A., & Smeets, M. (2020). Military Operations in Cyberspace. In A. M. Sookermany (Ed.), *Handbook of Military Sciences* (pp. 1–16). Springer International Publishing. https://doi.org/10.1007/978-3-030-02866-4_19-1

Brockmann, K., & Raju, N. (2022). *NewSpace and the Commercialization of the Space Industry: Challenges for the Missile Technology Control Regime*. SIPRI. https://www.sipri.org/publications/2022/other-publications/newspace-and-commercialization-space-industry-challenges-missile-technology-control-regime (accessed 22.08.2023)

Brunkard, P. (2021, July 12). The Space Wide Web Is Ready To Launch. *Forrester*. https://www.forrester.com/blogs/the-space-wide-web-is-ready-to-launch/ (accessed 19.02.2024)

Collier, R. (2017). NHS ransomware attack spreads worldwide. *CMAJ : Canadian Medical Association Journal*, *189*(22), E786–E787. https://doi.org/10.1503/cmaj.1095434

Components of a Satellite. (n.d.). *Space Foundation*. https://www.spacefoundation.org/space_brief/satellite-components/ 23.01.2023)

Computer Security Resource Center. (n.d.). *Cyberspace capability—Glossary | CSRC*. National Institute of Standards and Technology. https://csrc.nist.gov/glossary/term/cyberspace_capability (accessed 20.12.2023)

Critchley, L. (2018, November 14). *An Introduction to the Sensors Used in Space*. AZoSensors. https://www.azosensors.com/article.aspx?ArticleID=1473 (accessed 17.01.2024)

Cyber security and Infrastructure Security Agency (CISA). (2022). *Securing the Software Supply Chain: Recommended Practices Guide for Developers*. https://www.cisa.gov/sites/default/files/publications/ESF_SECURING_THE_SOFTWARE_SUPPLY_CHAIN_DEVELOPERS.PDF (accessed 14.02.2024)

Department of the Army. (2014). *Cyber Electromagnetic Activities* (Field Manual No. 3-38 FM 3-38). United States Army. https://irp.fas.org/doddir/army/fm3-38.pdf

Dinstein, Y., & Dahl, A. W. (2020). *Oslo Manual on Select Topics of the Law of Armed Conflict: Rules and Commentary*. Springer International Publishing. https://doi.org/10.1007/978-3-030-39169-0

Dolman, E. (2022) Space is a Warfighting Domain, Æther: A Journal of Strategic Airpower and Spacepower 1(1) Spring 2022, pages 82-90 https://www.airuniversity.af.edu/Portals/10/AEtherJournal/Journals/Volume-1_Issue-1/11-Dolman.pdf (accessed 03.09.2024)

The Norwegian Directorate for Civil Protection (DBS). (2016). *Samfunnets kritiske funksjoner—Hvilken funksjonsevne må samfunnet opprettholde til enhver tid?* (ISBN: 978-82-7768-412-3; Temarapport). Direktoratet for samfunnssikkerhet og beredskap. https://www.dsb.no/globalassets/dokumenter/rapporter/kiks-2_januar.pdf

Earth Science Data Systems, N. (2022, January 4). *Sensors* [Section Landing]. Earth Science Data Systems, NASA. https://www.earthdata.nasa.gov/sensors (accessed 28.09.2023)

Eide, K. A. (2023). *Space – det 5. operasjonsdomenet: En styrkemultiplikator for Hærens kampkraft?* Master thesis at Norwegian Defense College (FHS). https://fhs.brage.unit.no/fhs-xmlui/handle/11250/3113084 (accessed 09.04.2024)

Erwin, S. (2024, August 12) *SpaceX launches two satellites for Arctic broadband mission,* Space News. https://spacenews.com/spacex-launches-two-satellites-for-arctic-broadband-mission/ (accessed 21.08.2024)

European Space Angency. (n.d.). *Space debris by the numbers*. Retrieved September 27, 2023, from https://www.esa.int/Space_Safety/Space_Debris/Space_debris_by_the_numbers (accessed 27.09.2023)

Falco, G. (2018, September 17). *The Vacuum of Space Cyber Security*. https://doi.org/10.2514/6.2018-5275

Falco, G. (2020). When Satellites Attack: Satellite-to-Satellite Cyber Attack, Defense and Resilience. In *ASCEND 2020*. American Institute of Aeronautics and Astronautics. https://doi.org/10.2514/6.2020-4014

Fidler, D. P. (2018, March 4). *Cybersecurity and the New Era of Space Activities*. Council on Foreign Relations. https://www.cfr.org/report/cybersecurity-and-new-era-space-activities (accessed 29.09.2023)

Flaherty, M. P., Samenow, J., & Rein, L. (2014, November 12). Chinese hack U.S. weather systems, satellite network. *The Washington Post*. https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e_story.html (accessed 23.12.2023)

Norwegian Ministry of Defense. (2024a). *Prop. 87 S (2023 –2024) Proposisjon til Stortinget (forslag til stortingsvedtak)Forsvarsløftet – for Norges trygghet: Langtidsplan for forsvarssektoren 2025–2036 -*.

Norwegian Ministry of Defense. (2024b, February 16). *Norge inn i multilateralt militært romsamarbeid*. Regjeringen.no. https://www.regjeringen.no/no/aktuelt/norge-inn-i-multilateralt-militart-romsamarbeid/id3025749/ (accessed 11.04.2024)

Norwegian Ministry of Defense (2020). *Prop. 14 S (2020-2021) Evne til forsvar—Vilje til beredskap: Langstidsplan for forsvarssektoren*. Det kongelige forsvarsdepartement. https://www.regjeringen.no/contentassets/81506a8900cc4f16bf805b936e3bb041/no/pdfs/prp202020210014000dddpdfs.pdf (accessed 11.04.2024)

Norwegian Ministry of Defense. (2016). *Prop. 151 S (2015-2016) Kampkraft og bærekraft: Langtidsplan for forsvarssektoren*. Det kongelige forsvarsdepartement. https://www.regjeringen.no/contentassets/a712fb233b2542af8df07e2628b3386d/no/pdfs/prp201520160151000dddpdfs.pdf (accessed 11.04.2024)

Norwegian Defense Staff. (2015). *Et forsvar i endring—Forsvarssjefens fagmilitære råd 2015*. Forsvaret. https://www.forsvaret.no/forskning/forskning-utvikling-ved-forsvarets-hogskole/institutt-for-forsvarsstudier/forskningsressurser/fagmilitaere-utredninger/2015%20Forsvarssjefens%20fagmilit%C3%A6re%20r%C3%A5d%20-%20Et%20forsvar%20i%20endring.pdf/_/attachment/inline/b0b115a2-cca3-46fa-abdb-ac65bdae0f77:7d47de97aef0998243151d9377a300fda77ab15f/2015%20Forsvarssjefens%20fagmilit%C3%A6re%20r%C3%A5d%20-%20Et%20forsvar%20i%20endring.pdf (accessed 11.04.2024)

Norwegian Defense Staff. (2019). *Forsvarets fellesoperative doktrine 2019* Forsvaret. https://fhs.brage.unit.no/fhs-xmlui/bitstream/handle/11250/2631948/FFOD%202019%20.pdf (ISBN: 978-82-93114-99-4).

Fortinet. (2023). *What is a Brute Force Attack? | Definition, Types & How It Works*. Fortinet. https://www.fortinet.com/resources/cyberglossary/brute-force-attack (accessed 13.02.2024)

Fritz, J. (2013). *Satellite hacking: A guide for the perplexed. 10*(1).

Graczyk, R., Esteves-Verissimo, P., & Voelp, M. (2021). *Sanctuary lost: A cyber-physical warfare in space*. https://doi.org/10.48550/ARXIV.2110.05878

Greig, J. (2022, January 4). *Viasat confirms report of wiper malware used in Ukraine cyberattack*. The Record. https://therecord.media/viasat-confirms-report-of-wiper-malware-used-in-ukraine-cyberattack (accessed 12.10.2023)

Greig, J. (2023, August 11). *NSA, Viasat say 2022 hack was two incidents; Russian sanctions resulted from investigation*. The Record. https://therecord.media/viasat-hack-was-two-incidents-and-resulted-in-sanctions (accessed 10.10.2024)

Harrison, T., Johnson, K., & Young, M. (2021). *Defense Against the Dark Arts in Space: Protecting Space Systems from Counterspace Weapons*. Center for Strategic and International Studies (CSIS) https://www.csis.org/analysis/defense-against-dark-arts-space-protecting-space-systems-counterspace-weapons (accessed 13.04.2023).

Hofoss, E., Aarønæs, L., Abrahamsen, T., & Tollefsen, D. (2023). *Forsvaret i verdensrommet* (Viten: Forskningsfaglig Magasin 1.2023). Norwegian Defence Research Establishment (FFI).

Holtet, J. A., & Hammerstrøm, M. (2023). Andøya Space. In *Store norske leksikon*. https://snl.no/And%C3%B8ya_Space (accessed 23.04.2024)

Johnson-Freese, J. (2017). *Space Warfare in the 21st Century: Arming the Heavens*. Routledge. ISBN: 978-1-138-69386-9

Kaminska, M., Shires, J., & Smeets, M. (2022). Tallinn Workshop Report: Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far). *Tallinn Workshop Report*, https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf (accessed 08.08.2023)

Kaushal, S. (2021). *Operationalising the Constrain Concept: Competing Below the Threshold* (RUSI Whitehall Report ISSN: 1750-9432). Royal United Services Institute for Defence and Security Studies (RUSI). https://static.rusi.org/310-Constrain-WHR.pdf

Klein, J. J. (2019). *Understanding Space Strategy: The Art of War in Space* (1st ed.). Routledge. https://doi.org/10.4324/9780429424724

Lehto, M. (2015). Phenomena in the Cyber World. In M. Lehto & P. Neittaanmäki (Eds.), *Cyber Security: Analytics, Technology and Automation* (pp. 3–29). Springer International Publishing. https://doi.org/10.1007/978-3-319-18302-2_1

Lin, H. (2012). Escalation Dynamics and Conflict Termination in Cyberspace. *Strategic Studies Quarterly*, *6*(3), 46–70.

Livingstone, D., & Lewis, P. (2016). *Space, the Final Frontier for Cybersecurity?* (International Security Department). Chatham House: The Royal Institute of International Affairs.

Lockheed Martin. (n.d.). *Cyber Kill Chain®*. Lockheed Martin. https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html (accessed 20.12.2023)

Loughran, J. (2018, June 20). *Chinese hacking operation uncovered; penetrated key satellite companies and more*. Engineering and Technology Magazine. https://eandt.theiet.org/2018/06/20/chinese-hacking-operation-uncovered-penetrated-key-satellite-companies-and-more (accessed 23.12.2024)

Lutkevich, B. (n.d.). *What is a Backdoor Attack? Tips for Detection and Prevention*. Tech Target. https://www.techtarget.com/searchsecurity/definition/back-door (accessed 21.02.2024)

Lutkevich, B. (2021, December). *What is a timestamp?* WhatIs Tech Target. https://www.techtarget.com/whatis/definition/timestamp (accessed 21.02.2024)

Lutkevich, B. (2022, July). *What is Access Control?* Security. https://www.techtarget.com/searchsecurity/definition/access-control (accessed 21.02.2024)

Manulis, M., Bridges, C., Harrison, R., Sekar, V., & Davis, A. (2021). Cyber security in New Space: Analysis of threats, key enabling technologies and challenges. *International Journal of Information Security*, *20*. https://doi.org/10.1007/s10207-020-00503-w

Marples, M. (2022, July 5). *NASA lost contact with a satellite after it broke free of the Earth's orbit*. CNN. https://www.cnn.com/2022/07/05/world/nasa-satellite-capstone-earth-orbit-scn/index.html (accessed 27.02.2024)

Martin, A.-S. (2023). Outer Space, the Final Frontier of Cyberspace: Regulating Cybersecurity Issues in Two Interwoven Domains. *Astropolitics*, *21*(1), 1–22. https://doi.org/10.1080/14777622.2023.2195101

McKay, T. (2023, September 12). *Hackers compete to break into the Space Force's Moonlighter satellite*. IT Brew. https://www.itbrew.com/stories/2023/09/12/hackers-compete-to-break-into-the-space-force-s-moonlighter-satellite (accessed 14.02.2024)

Meyers, J. S., & Kazil, J. (2023, November 7). How to 'harden' open-source software. *Binding Hook*. https://bindinghook.com/articles-binding-edge/how-to-harden-open-source-software/ (accessed 21.12.2023)

Mhackeroni, (finalist team name). (2023, September). *Hack-A-Sat 4 Finalist Tech Papers*. GitHub. https://github.com/cromulencellc/hackasat-finals-2023/tree/main/team_writeups (accessed 14.02.2024)

Moore, D. (2022). *Offensive cyber operations: Understanding intangible warfare*. Hurst & Company. ISBN: 978-1-78738-561-0

NASA Office of Inspector General. (2019). *Cybersecurity Management and Oversight at the Jet Propulsion Laboratory* (Technical Report IG-19-022). National Aeronautics and Space Administrategion (NASA). https://oig.nasa.gov/docs/IG-19-022.pdf

NATO. (2022, January 17). *NATO's overarching Space Policy*. NATO. https://www.nato.int/cps/en/natohq/official_texts_190862.htm (accessed 11.04.2024)

NATO Allied Joint Publications. (2020). *AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (Edition A)*. Nato Standardization Office. https://assets.publishing.service.gov.uk/media/5f086ec4d3bf7f2bef137675/doctrine_nato_cyberspace_operations_ajp_3_20_1_.pdf

Norwegian Space center (Norsk romsenter). (n.d.). *Satellitter, infrastruktur og statlige romaktører*. Norsk Romsenter. from https://romsenter.no/satellitter-infrastruktur-og-statlige-romaktoerer (accessed 11.04.2024)

Northorp Grumman. (2021, September 16). *Northrop Grumman's LEO Satellite Payload for DARPA Revolutionizes Positioning, Navigation and Timing*. Northrop Grumman Newsroom. https://news.northropgrumman.com/news/releases/northrop-grummans-leo-satellite-payload-for-darpa-revolutionizes-positioning-navigation-and-timing (accessed 17.01.2024)

Norwegian Ministry of Trade, Industry and Fisheries. (2019). *Meld. St. 10 (2019-2020) Høytflyvende satelitter, jordnære forhold: En strategi for norsk romvirksomhet* (Meld. St. 10 (2019-2020)).

Norwegian Ministry of Trade, Industry and Fisheries, (2006, November 28). *Norsk Romsenter (NRS)*. Regjeringen.no https://www.regjeringen.no/no/dep/nfd/org/etater-og-virksomheter-under-narings--og-fiskeridepartementet/Subordinate-agencies-and-institutions/norsk-romsenter-nrs/id435114/ (accessed 23.03.2024).

O'Connor, S.E. (2022). Managing the Cyber-Related Risks to Space Activities. In: Pozza, M.A., Dennerley, J.A. (eds) Risk Management in Outer Space Activities. Space Law and Policy. Springer, Singapore. https://doi.org/10.1007/978-981-16-4756-7_6

Oladimeji, S., & Kerner, S. M. (2023, November 3). *SolarWinds hack explained: Everything you need to know*. Tech Target. https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (accessed 14.02.2024)

Olsen, R. (2017). *– Norge trenger et nasjonalt romprogram*. https://www.ffi.no/aktuelt/arrangementer/-norge-trenger-et-nasjonalt-romprogram (accessed 16.02.2024)

Our World in Data. (n.d.). *Annual number of objects launched into space*. Our World in Data. Retrieved October 12, 2023, from https://ourworldindata.org/grapher/yearly-number-of-objects-launched-into-outer-space?facet=none

Paikowsky, D. (2017). What Is New Space? The Changing Ecosystem of Global Space Activity. *New Space*, *5*(2), 84–88. https://doi.org/10.1089/space.2016.0027

Pavur, J., & Martinovic, I. (2019). The Cyber-ASAT: On the Impact of Cyber Weapons in Outer Space. *2019 11th International Conference on Cyber Conflict (CyCon)*, *900*, 1–18. https://doi.org/10.23919/CYCON.2019.8756904

Pavur, J., & Martinovic, I. (2021). On Detecting Deception in Space Situational Awareness. *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 280–291. https://doi.org/10.1145/3433210.3453081

Pavur, J., & Martinovic, I. (2022). Building a launchpad for satellite cyber-security research: Lessons from 60 years of spaceflight. *Journal of Cybersecurity*, *8*(1), tyac008. https://doi.org/10.1093/cybsec/tyac008

Pavur, J., Strohmeier, M., Lenders, V., & Martinovic, I. (2021). In the Same Boat: On Small Satellites, Big Rockets, and Cyber Trust. *2021 13th International Conference on Cyber Conflict (CyCon)*, 151–169. https://doi.org/10.23919/CyCon51939.2021.9468300

Perlroth, N. (2021). *This is how they tell me the world ends: The cyberweapons arms race*. Bloomsbury Publishing. ISBN: 978-1-63557-605-4

Poirier, C. (2022). *The War in Ukraine from a Space Cybersecurity Perspective* (ISSN: 2076-6688). European Space Policy Institute (ESPI). https://www.espi.or.at/wp-content/uploads/2022/10/ESPI-Short-1-Final-Report.pdf

Prague Security Studies Institute (2018) Europe's Preparedness to Respond to Space Hybrid Operations https://www.pssi.cz/download//docs/8252_597-europe-s-preparedness-to-respond-to-space-hybrid-operations.pdf accessed 12.09.2020

Rajagopalan (2019) Electronic and Cyber Warfare in Outer Space, Space Dossier 3, May 2019, The United Nations Institute for Disarmament Research (UNIDIR), https://unidir.org/publication/electronic-and-cyber-warfare-in-outer-space/ Accessed 03.09.2024

Rid, T., & Buchanan, B. (2015). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382

Robinson, J. (2016). *Governance challenges at the intersection of space and cyber security*. The Space Review. https://www.thespacereview.com/article/2923/1 (accessed 08.06.2023)

Sanchez, & Zatti. (2020). *Handbook of Space Security* (K.-U. Schrogl, Ed.; Second edition). Springer. https://doi.org/10.1007/978-3-030-23210-8

Santamarta, R. (2014). *SATCOM Terminals: Hacking by Air, Sea, and Land* [Technical White Paper]. Black Hat.

Santamarta, R. (2018). *Last Call for SATCOM Security—White paper*. IO Active. https://i.blackhat.com/us-18/Thu-August-9/us-18-Santamarta-Last-Call-For-Satcom-Security-wp.pdf

Satellite Turla: APT Command and Control In the Sky. (2015, September 9). *SecureList APT Reports*. https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/ (accessed 23.12.2023)

Schneider, J. G. (2019). Deterrence in and through Cyberspace. In E. Gartzke & J. R. Lindsay (Eds.), *Cross-Domain Deterrence: Strategy in an Era of Complexity* (p. 0). Oxford University Press. https://doi.org/10.1093/oso/9780190908645.003.0005

Sgobba, T., & Allahdadi, F. A. (2013). Chapter 8—Orbital Operations Safety. In F. A. Allahdadi, I. Rongier, & P. D. Wilde (Eds.), *Safety Design for Space Operations* (pp. 411–602). Butterworth-Heinemann. https://doi.org/10.1016/B978-0-08-096921-3.00008-8

Singer, P. W., & Wood, P. (2021, May 26). *Keep Tabs on China's Growing Space Situational Awareness*. Defense One. https://www.defenseone.com/ideas/2021/05/keep-tabs-chinas-growing-space-situational-awareness/174309/ (accessed 11.10.2023)

Smeets, M., & Soesanto, S. (2020, February 18). *Cyber Deterrence Is Dead. Long Live Cyber Deterrence!* Council on Foreign Relations. https://www.cfr.org/blog/cyber-deterrence-dead-long-live-cyber-deterrence (accessed 20.12.2022)

Smeets, Max (2017) *Europe Slowly Starts to Talk Openly About Offensive Cyber Operations*. Council on Foreign Relations. https://www.cfr.org/blog/europe-slowly-starts-talk-openly-about-offensive-cyber-operations (accessed 30.09.2022)

Space Norway. (n.d.). *Milepæler | HEOSAT*. Space Norway. https://spacenorway.no/en/heosat/milestones/ (accessed 12.04.2024)

Splunk Threat Research Team. (2022, May 19). *Threat Update: AcidRain Wiper*. Splunk-Blogs. https://www.splunk.com/en_us/blog/security/threat-update-acidrain-wiper.html (accessed 12.10.2023)

Stevens, T. (2012). A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy*, *33*(1), 148–170. https://doi.org/10.1080/13523260.2012.659597

Sundlisaeter, T. (2022). *Space Power in the High North—Persepctives from the Kingdom of Norway* PhD Dissertation from University of St. Andrews. https://research-repository.st-andrews.ac.uk/bitstream/handle/10023/26378/Thesis-Tale-Sundlisaeter-complete-version.pdf?sequence=7&isAllowed=y

Swope, C., Bingen, K. A., Young, M., Chang, M., Songer, S., & Tammello, J. (2024). *Space Threat Assessment 2024* (CSIS Aerospace Security Project). Center for Strategic and International Studies (CSIS). https://csis-website-prod.s3.amazonaws.com/s3fs-public/2024-04/240417_Swope_Space_Threat_0.pdf?VersionId=DDeJ0EkYnF5W7POfMJHVGjkxEVeTx3o0 (accessed 03.09.2024)

Thangavel, K., Plotnek, J. J., Gardi, A., & Sabatini, R. (2022). Understanding and investigating adversary threats and countermeasures in the context of space cybersecurity. *2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC)*, 1–10. https://doi.org/10.1109/DASC55683.2022.9925759

The Consultative Committee for Space Data Systems. (2021). *TM Space Data Link Protocol—Recommendations for Space Data System Standards* (Recommended Standard CCSDS 132.0-B-3). The Consultative Committee for Space Data Systems. https://public.ccsds.org/Pubs/132x0b3.pdf

The European Space Agency. (n.d.). *SSA Programme overview*. European Space Agency Official Website. https://www.esa.int/Space_Safety/SSA_Programme_overview (accessed 19.02.2024)

The International Telecommunication Union. (n.d.). *The International Telecommunication Union Official website*. ITU. https://www.itu.int:443/en/Pages/default.aspx (accessed 13.10.2023)

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

Thorpe, E. (2022, March 28). *Satellites Orbits: Types & Uses Explained*. Orbital Today. https://orbitaltoday.com/2022/03/28/satellites-orbits-types-uses-explained/ (accessed 19.02.2024)

Thorton, W. (2023, November 15). *Differences Between GNSS and PNT*. Spirent. https://www.spirent.com/blogs/whats-the-difference-between-gnss-and-pnt (accessed 17.01.2024).

Thummala, R. (2023). Space Worms: On the Threat of Cyber-ASAT Weaponry to Satellite Constellations Master’s Thesis at Penn State University. https://www.researchgate.net/publication/372310903_Space_Worms_On_the_Threat_of_Cyber-ASAT_Weaponry_to_Satellite_Constellations (accessed 10.11.2023)

United Nations Office for Outer Space Affairs. (1967). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty)* (Resolution Adopted by the General Assembly 2222 (XXI)). United Nations Office of Outer Space Affairs (UNOOSA). https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/outerspacetreaty.html (accessed 02.02.2024)

US Department of Commerce Office of the Inspector General. (2014). *Expedited Efforts Needed to Remediate High-Risk Vulnerabilities in JPSS Ground System.* (Technical Report OIG-14-027-M). United States Department of Commerce Office of the Inspector General. https://www.oig.doc.gov/OIGPublications/OIG-14-027-M.pdf

U.S. Joint Chiefs of Staff. (2017). *Joint Operations* (Joint Publication 3-0 JP 3-0). Joint Chiefs of Staff. https://irp.fas.org/doddir/dod/jp3_0.pdf

Van Puyvelde, D., & Brantly, A. F. (2019). *Cybersecurity: Politics, Governance and Conflict in Cyberspace*. Polity Press.

White, M. (2020, July 14). *Middle East braces itself for cyber warfare*. Global Trade Review (GTR). https://www.gtreview.com/magazine/volume-18-issue-3/middle-east-braces-cyber-warfare (accessed 18.06.2024)

World economic forum. (2022, May 25). *Why we need increased cybersecurity for space-based services*. World Economic Forum. https://www.weforum.org/agenda/2022/05/increased-cybersecurity-for-space-based-services/ (accessed 29.09.2023)

Zilincik, S., & Duyvesteyn, I. (2023). Strategic studies and cyber warfare. *Journal of Strategic Studies*, *46*(4), 836-857. https://doi.org/10.1080/01402390.2023.2174106

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's mission

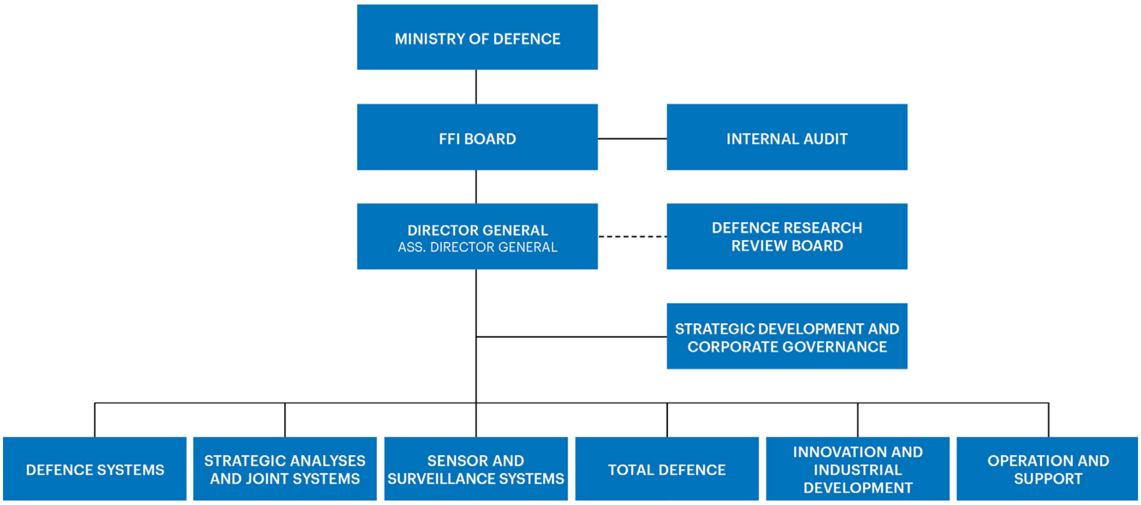
FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's vision

FFI turns knowledge and ideas into an efficient defence.

FFI's characteristics

Creative, daring, broad-minded and responsible.


MINISTRY OF DEFENCE
FFI BOARD
INTERNAL AUDIT
DIRECTOR GENERAL
ASS. DIRECTOR GENERAL
DEFENCE RESEARCH REVIEW BOARD
STRATEGIC DEVELOPMENT AND CORPORATE GOVERNANCE
DEFENCE SYSTEMS
STRATEGIC ANALYSES AND JOINT SYSTEMS
SENSOR AND SURVEILLANCE SYSTEMS
TOTAL DEFENCE
INNOVATION AND INDUSTRIAL DEVELOPMENT
OPERATION AND SUPPORT

Forsvarets forskningsinstitutt (FFI)
Postboks 25
2027 Kjeller

Besøksadresse:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telefon: 91 50 30 03
E-post: post@ffi.no
ffi.no

Norwegian Defence Research Establishment (FFI)
PO box 25
NO-2027 Kjeller
NORWAY

Visitor address:
Kjeller: Instituttveien 20, Kjeller
Horten: Nedre vei 16, Karljohansvern, Horten

Telephone: +47 91 50 30 03
E-mail: post@ffi.no
ffi.no/en