arXiv:2110.05878v1 [cs.CR] 12 Oct 2021

Sanctuary lost: a cyber-physical warfare in space

Rafal Graczyk*, Paulo Esteves-Verissimo†, and Marcus Völp*
*University of Luxembourg, Interdisciplinary Center for Security, Reliability and Trust (SnT) - CritiX group
†King Abdullah University of Science and Technology (KAUST), Resilient Computing and Cybersecurity Center (RC3)
*{rafal.graczyk, marcus.voelp}@uni.lu †paulo.verissimo@kaust.edu.sa

***Abstract*—Over the last decades, space has grown from a purely scientific struggle, fueled by the desire to demonstrate superiority of one regime over the other, to an anchor point of the economies of essentially all developed countries. Many businesses depend crucially on satellite communication or data acquisition, not only for defense purposes, but increasingly also for day-to-day applications. However, although so far space faring nations refrained from extending their earth-bound conflicts into space, this critical infrastructure is not as invulnerable as common knowledge suggests. In this paper, we analyze the threats space vehicles are exposed to and what must change to mitigate them. In particular, we shall focus on cyber threats, which may well be mounted by small countries and terrorist organisations, whose incentives do not necessarily include sustainability of the space domain and who may not be susceptible to the threat of mutual retaliation on the ground. We survey incidents, highlight threats and raise awareness from general perparedness for accidental faults, which is already widely spread within the space community, to preparedness and tolerance of both accidental and malicious faults (such as targeted attacks by cyber terrorists and nation-state hackers).**

***Index Terms*—space, satellite, cyberphysical, system, threat vector, cybersafety, cybersecurity**

I. INTRODUCTION

Space infrastructure in itself is not a very large business: with 366 billion USD of global revenues [1], it constitutes ∼0.42% of the global economy of 87.5 trillion USD in 2019 [2], [3].

Space assets used to be of military origin, since the 80's of XX century, are increasingly civilian, starting from telecommunications, then spreading to other fields of near space exploitation. Today, many other sectors of our economy, even if, apparently ground-based, crucially depend on the space infrastructure, including [4]: mass media, global transport and logistics, military, intelligence, utilities, agriculture, banking, oil and mining. Activities from private companies such as SpaceX with Starlink and OneWeb complement this list with megaconstellations providing communication and fast internet to remote locations.

This dependence turns space into an important resource, in particular for the developed countries and their economies, space faring and not, and a worthwhile target for protection. Unfortunately several threats put the sustainable use of space at risk, both as a foundation for military operations, but more importantly for the economic applications that affect our daily life.

In this paper, we review past incidents and derive a comprehensive threat-plane for space and the orbits therein as sustainable resource to deploy satellites for a multitude of purposes, but also for human and robotic scientific missions. We consider both threats from accidental causes, but more importantly also threads originating from intentionally malicious activities, such as targeted cyber and/or physical attacks.

As we shall see, threats do not only originate from other space-faring nations and their ability to damage, shoot down or disrupt communication of other space-faring nation's vehicles. They may also originate from terrorist groups and the nation-state hackers of less developed countries who would not suffer from disrupting access to space for the upcoming decades until effective debris-removal technologies become available. In particular, not all of these groups are vulnerable to the common threat of retaliation on the ground, which several space faring nations formulated as balance of powers, should space vehicles of that nation be attacked. Even the correct attribution of attacks will be difficult, as can be seen in some of the recent cyber attacks that keep happening on ground.

We assume this topic may as well be interesting for a lay audience, not necessarily proficient in the details of space flight or in the way cyber attacks can manifest. In addition to our threat-plane analysis, we shall therefore also introduce the background necessary for understanding these aspects, inviting the proficient reader to skip these sections. Our contributions include in Section III an analysis why space forms a critical information infrastructure worth protecting, a taxonomy of kinetic and non-kinetic threats space vehicles are exposed to (in Section IV), which we shall apply in our survey of past incidents during the various stages of space vehicle development, deployment and operation (in Section VI). Where appropriate, we suggest measures which may help overcome some of these threats, however ultimately we recommend leveraging on the care already taken to tolerate, survive and repair the consequences of accidental faults and to extend this care to also become resilient to intentionally malicious faults. We begin by surveying space flight and the foundations on which it is based.

II. SPACE FLIGHT 101

Any projectile (ball, rock, axe) thrown at ground level, tangential to a planet's surface, will closer or farther fall down. That's what everyday experience tells us and this intuition is generally true, unless the projectile is thrown so fast that it falls at the same rate, that the ground recedes. The Earth is a geoid. However, for our little thought experiment we approximate it to be spherical, receding roughly 5 meters for every 8 km traveled along the tangent. The exact speed, required for maintaining the hypothetical trajectory, following planet's surface, depends on the planet's mass and is called first cosmic velocity. For Earth, this velocity is roughly 7.9 km/s.

Changing in our experimental setup the projectile to a satellite, our throwing hand to a rocket and raising the target altitude to above the atmosphere, where there are no buildings, hills, weather and last, but most importantly, no atmospheric drag, and we have entered the space domain and successfully placed our satellite on a path called the orbit.

Raising the orbit's altitude, we reduce the velocity required to maintain a circular orbit (one with the same altitude above Earth at all times). At the same time, we increase the orbital period, which at low Earth orbits (LEOs) is about 90 minutes. Orbital period is the time after which a satellite returns to the same position above ground, here after 1.5 hours, not yet compensating for the rotation of the Earth.

Observers on the ground will still notice the satellite several hundreds if not thousands of kilometers west, although the spacecraft returned to its initial position. This is because our planet rotates at a linear velocity of 1670 km/h at the equator, which decreases as the latitude increases (e.g., to 1180 km/h at 45 degrees and to 0 km/h at the Poles, at 90 degrees). For satellite operators this implies limited visibility of the satellite and hence also limited communication possibilities. Sometimes, depending on the exact location of the ground station relative to the satellite's orbit, convenient revisits may happen only after days.

A satellite's orbiting plane can be oriented in all possible angles with respect to the Earth's rotation plane. Orbital planes can be equatorial, so that satellites will travel over the equator, or they can be more inclined, allowing satellites to visit (observe/ communicate with) higher latitudes, up to polar orbits where satellites will fly over each of the Earth's poles.

As mentioned before, the higher the altitude of a satellite's orbit, the longer its orbital period. At roughly 36,000 km above Earth (about 10 % of the distance to the Moon), the orbital period becomes almost 24 hours, the same length as Earth's rotation period. Satellite on such an orbit are geosynchronous and will visit each place on its path at exactly the same time of day. If geosynchronous orbits have an inclination of zero degrees with respect to the equator, the orbit becomes geostationary and satellites on this orbit stand still over the same place on Earth, as they have the same angular velocity as the Earth rotating below them. As this happens 36000 km above the Earth's surface, the whole planet's hemisphere can be in view, which is a neat feature for telecommunication or observation purposes, with obvious drawbacks caused by the distance from ground that these satellites must have: the propagation of radio signals causes noticeable latency and very sophisticated optical and attitude stabilization systems are needed to maintain accurate satellite pointing. Typical orbits and their applications are summarized in Table I.

A. *Fuel and Power Considerations*

Satellites above the atmosphere operate in vacuum, which very quickly becomes very deep and provides so little residual atmospheric drag that for precise satellite modeling purposes, other factors begin to dominate, such as the influence of solar radiation.

Satellites and probes do not necessarily need propulsion to stay on orbit or to maneuver and change attitude. This is obviously a bit of a too idealistic take on orbital mechanics, as non-homogeneity of the gravitation field, influence of other celestial bodies, solar wind and pressure, changes of the residual atmospheric drag (e.g., due to high Sun activity), etc., perturb the stability of the orbit, both in its plane arrangement and in its altitude. In most parts however, it can be assumed that bodies injected into a stable orbit will stay on this orbit and that changing the orbit requires some kind of propulsion, such as rocket engines, cold gas thrusters, resitojet thrusters, and various kinds of electric engines (e.g., ion or Hall effect).

While particular implementations may vary significantly, generation of thrust requires mass to be ejected for the spacecraft to experience a force in the opposite direction. The bigger the mass times its ejection velocity, the bigger will be the force that acts upon the spacecraft and also the acceleration that the spacecraft experiences in the direction of this force.

Stored fuel and the spacecraft's propulsion capacity to change it's velocity thus define how fast the craft can change its orbit and ultimately constrains its mission and the maneuvers it can execute during that time.

Some changes of the orbit require only reasonable amounts of fuel, especially raising and lowering the perigee or the apogee of an orbit(i.e., the point closest to / farthest from the Earth's center). Both points can be adjusted using Hohmann maneuvers, which require engine burns tangential to the orbit in one of these points to affect the opposite one (for details refer to [9], [10], [11], [8]). Other maneuvers are more demanding and thus affect mission time more severely. For example, changing the inclination of a satellite requires redirecting its momentum, most of which has been built up at the launch and with the launch vehicle's propulsion. Not many of these maneuvers can be performed with the limited fuel and propulsion capacity of the satellite. Spacecraft injected by its launch vehicle or by its apogee motor into an orbit are therefore typically left in this orbit. Apogee motors are typically found in GEO satellites to make the orbit circular. Space plane concept, which theoretically, could help to overcome satellite maneuverability limitations, at the time of writing of this paper, is very immature technology in practice [12], [13].

Spacecraft are also very constrained on the side of (electrical) power supply. In practice, there are two primary power sources - solar arrays (suitable for use in inner Solar System, beyond Mars, up to asteroid belt) and radioisotope thermoelectric generator (RTG). Solar arrays take sunlight and convert (up to 30-35% of it) into electric power. Solar arrays in order to reach higher power output need to occupy large

Type	Altitude [km]	Remarks
VLEO Very Low Earth Orbit	180 - 500	Earth observation (EO), very low communication latency; high imaging resolution with mildly sophisticated equipment; atmospheric drag causes the satellite to require propulsion to maintain the altitude; operation altitude of the International Space Station (ISS)
LEO Low Earth Orbit	500 - 2000	EO, low communication latency; popular for microsatellites
SSO Sun-Synchronous Orbit	same as LEO	subtype of LEO; low, retrograde orbit, sun synchronous; revisits the same spot at the same tame of day (the same shadows cast by objects), used for observation satellites; if traveling along the terminator line (dawn-dusk orbit) satellite could spent majority of time in sunlit conditions — a preferable arrangement for power constrained satellites
MEO Medium Earth Orbit	2000 - 35786	used by Global Navigation Satellite Systems (GNSS) systems, some telecommunication constellations(i.e. SES O3b)
HEO Highly Elliptical Orbit	perigee and apogee vary	highly elliptical orbit, used for communication satellites or science equipment
GTO Geo Transfer Orbit	perigee and apogee vary	subtype of HEO; used for accessing GEO and beyond (cis-lunar space, lunar orbits and deeper into the Solar System)
GEO Geosynchronous Orbit	35786	telecommunication and observation satellites, if over equator, is Geostationary Orbit
GEO Graveyard	∼36300	decommissioned GEO satellites shall end up here

TABLE I
SUMMARY OF MOST POPULAR ORBITS AND THEIR APPLICATIONS [5], [6], [7], [8]

areas which requires them to be deployable (they have to reliably unfold), which in turn makes the attitude control more challenging. RTG's require heatsinks which are dead mass which increases the launch cost, not to mention, that application of this technology is limited by environmental and political constraints [14], [15].

To sum up, both, electrical power, for supplying the spacecraft, and fuel, for managing the spacecraft orbit, are ultimate currencies in which each spacecraft designer and operator has to pay for owned vessel functions and capabilities. Since the spacecraft design and operation concepts are the results of a long and tedious process of architectural trade-offs it is usually very hard to add new function to already operating systems or to maneuver them in way that was not foreseen in the first place. Since placement in orbit, spacecraft is bound to follow it's preconceived destiny and the margins that could be used for changing mission objectives are minimal, and, typically, are left for emergency or fault contingency operations.

B. *On Board Systems*

Space systems operate in the harsh environment of outer space, remotely and, during times when no direct connection with ground stations is possible, with limited supervision. In addition to operating the instruments required to fulfill the satellites mission (sensors, cameras, communication relays, etc.), which are called the payload part, the satellite must also secure its own survival over the envisioned mission time and beyond. Despite shorter initially foreseen lifetimes (e.g., of a few months on low orbit, a few years for regular satellites or 15 years for GEO), due to limitations outlined in Section II-A, satellite lifetimes can go far beyond this initial plan (e.g., 20 years and counting for the ISS [16] and 43 years and counting for the two of Voyager spacecraft [17]).

The platform part assumes this role of securing a satellite survival. More precisely, it ensures sufficient resources remain available for the payload systems to fulfill their mission. The platform also controls power & thermal management, propulsion and thus orbit and attitude control as well as the command and telemetry links .

Depending on the type of mission, payloads might require more or less supervision, may have own communication links (both, up- and down-links), but are otherwise isolated from the platform part. The platform supplies the payload system with resources, commands and receives telemetry in return. In all other aspect, the platform remains separate from the payload subsystem, as its ultimate role is to ensure the operational safety of the satellite as a whole.

C. *Space Systems beyond Space*

Space operations consist not only of the vehicles deployed in space (satellites, stations, spacecraft), but also include systems on the ground for operation planning, control, tracking and communication, as well as the launch vehicles required to deploy spacecraft in space. The segments are called space, ground and launch segment, respectively. Ground segment, consists mainly of ground stations (used to establish communication with spacecraft platform, payload or both) and mission control facilities where commanding of spacecraft takes places. Tracking facilities, used to be assumed as a part of ground segment, but nowadays, due to significant increase in space congestion, traffic management becomes recognized as another, independent, segment of space system architecture. Here, we shall return to specifics of the ground-space interactions outlined at the beginning of this chapter, and remind that any ground based facility is limited in it's capability to establish communication with (or track) the satellite. Likewise, satellite is able to interact (i.e. provide the service) with entities withing it's field of view, during the time of pass (with the obvious advantage of geostationary satellites having constant field of view and capacity to provide a continuous service). Hence, the ground-space interaction limitations impose that:

1) With a few exceptions, ground stations lose contact once the satellite leaves their observation cone. Unless the provider has access to geographically spread ground stations to continuously track the satellite, the vehicle must operate autonomously; and
2) Having observed the satellite, adversaries may predict when it comes into range of a critical operation to conceal their activity or to take countermeasures against the satellite.

In addition, there is so called user segment, which consists of user terminals for telecommunication services [18] but also satellite navigation receivers [19], AIS [20] or ADS-B [21] transmitters or other, similar, systems. Organizations, facilities and infrastructure that is used to process or distribute acquired information to interested parties are also considered as a part of user segment.

D. *Crewed vs Robotic*

So far we discussed mainly about satellites, but spacecraft can be capable of supporting human space flight. Main differences between crewed and robotic activities, are the stakes (loss of life vs loss of equipment), complexity (life support systems and operations), capabilities (crewed missions are much more flexible as utilize human invention) and purpose (robotic are there to build infrastructure for services or explore deep space, while crewed are for science, outreach). While crewed operations are, for the time being, limited to few stations orbiting the Earth on LEO [16], [22], this is expected to change in the near feature with human expansion to cislunar space [23], following the scientific steps of Apollo program [24] and building foundations for sustained human presence beyond Earth and extending technical and economic activity to other celestial bodies. Today, crewed missions are primarily limited to science missions and sophisticated repairs where human flexibility to react to unforeseen situations outweighs the additional weight and complexity of life-support systems and the higher risks of the mission. Whereas loss of equipment is an unfortunate but tolerable event, loss of life remains unacceptable.

E. *Life cycle*

A peculiar aspect of space systems is the length of their life cycle and associated costs. The time from conception and preliminary design to the disposal of the first unit of a future space system (be it a satellite or a spacecraft) can easily span 2 or more decades. The last units remaining in operation can be decommissioned after 3-4 decades since the time they were designed.

This has several reasons: First, space projects are managed by large governmental agencies which aim to minimize project organizational and technical risks by enforcing bureaucratic processes and adherence to space, industrial, standards [25], [26] which typically require extensive documentation of the work done and planned. While justified for crewed missions or high profile missions, these processes are not always necessary for shorter, cheaper, experimental missions, which is the trend already visible in the community and is described in greater details in following section II-F. Stretching the design process in time increases the costs of a mission, in particular in terms of the staff required to follow these processes.

Second, design processes are limited to equipment that is built exclusively from qualified components, which are carefully tested for their suitability for space. Component qualification involves a significant number of tests, many of which lead to the destruction of the units under test, and require careful documentation. Again labor intensive tasks have to be conducted for the purpose of providing assurance to customers or stakeholders.

Third, these costs and manpower needs are further magnified by several levels of subcontracting and can easily lead to a price factor of 10–100 compared to commercial of the shelf (COTS) equipment or component that is not space graded.

A fourth aspect worth considering in the space segment life cycle, is that changes to already established and qualified designs nullifies the qualification status of this design and requires repeating the above processes. Shortcuts in the form of so called delta-qualifications are only possible if the change is small and still requires re-testing of all critical aspects related to that change.

This has two consequences:

1) Due to the high costs of the qualification process, new equipment gets subjected to it only if the additional performance justifies such expenses; and
2) Due to the time needed, space graded equipment often lags 10–15, or more, years behind COTS equipment.

We shall return to this when reflecting about the threats to which spacecrafts are exposed.

F. *New Space*

A careful reader will by now already have spotted vulnerabilities due to inefficiencies in the classical way of development and deployment of space vehicles and the infrastructure they need on the ground. Let us therefore also introduce a recent trend towards a more lean process for building space infrastructure, whose risks and threats we will analyze as well: *NewSpace* [27].

The NewSpace movement gains popularity due to its promise of more affordable satellites and launchers. NewSpace aims to build upon COTS technologies and components that, if qualified at all, undergo a much more relaxed testing regime [28], [29], accepting higher risks of failure for the sake of improved performance. The promise of NewSpace applies in particular to LEO, where harsh environmental influence is present, but weaker, than in higher orbits.

While by no doubt, the trend is clear and hundreds of new companies have already entered this market, which, as of 2020, grew to 26.2 BUSD invested in space start-ups since 2015 (at the scale of 36.7 BUSD invested since 2000) [30]. That is truly enormous progress, but there are also few downsides of such fast paced development process–the number of small satellites (from sub-kg to 600 kg of mass) launched every year, since 2017, is more than three hundred [31] and is increasing, from 2010 to 2020, number of actively operating satellites has grown 252% [32].

NewSpace in it's dynamics and consequences is a process of rapid economic expansion and unbounded exploitation of resources, very similar to examples on Earth, which have lead to overexploitation and environmental devastation. Outer space, especially LEO, used to be free of debris, but is now populated by a large number of new spacecrafts entering into service, sometimes even from a single launch, with debris (primarily from upper stage operations) starting to accumulate beyond tolerable dimensions.

Increasing orbital congestion combined with a general disregard of long term sustainability of the space environment (i.e. failure to ensure fast deorbiting when satellites are disposed) are first steps towards Kessler's syndrome [33] and we still have no capacity to purge orbits from dead satellites and debris.

Reduced costs also originate from higher turnaround times of a few month between contract signature and orbit injection rather than years. The lower costs and simplified quality assurance results in, higher, than in Old Space, mission failure rates. For example, Jacklin [34] found that around 40% of all small satellite mission launched between 2009 and 2016 failed partially or fully. It is also worth mentioning that Jacklin excluded academic endeavors from this analysis as their success if often defined very broadly. It is also fair to indicate that further industrialization of processes in NewSpace domain will reduce expected failure rates, as it is already seen with Starlink, trending towards 3% failure rate [35]. However, special care must be exercised to not let the same time-to-market mechanisms that are also present in other weakly regulated fields cause security to be treated as an aftermath.

NewSpace is on course of enabling satellites to become interconnected, creating orbital networks with many nodes and numerous points of entry that are eventually connected to the Internet. It leads to the creation of (mega-)constellations (i.e., formations of spacecrafts cooperating in achieving a common goal, typically for telecommunication but also for real-time Earth observation and similar activities [36]), which on the one hand enables operators and users to utilize the greater potential of these new services and increases the availability and robustness against accidental faults. At the same time, NewSpace approach, and use of large constellations in particular, also increases the attack surface, making it harder to defend and maintain control on the system. The trend of increasing the size of satellite constellation along with simplifying and miniaturizing the satellites themselves starts to spill into the traditional space industry [37], and most likely will become even more significant in the future.

G. Space sustainability

In Section II-F we have already mentioned that space near Earth, especially LEO, is exploited beyond it's capacity to naturally clean itself from dead spacecraft and launch and deployment debris (not to mention fields of debris resulting from collisions). The Kessler syndrome [33] is an existential threat to humankind capability to use space as part economy and explore space as a part of our destiny. In 2021, caused, by both extensive utilization and debris creation, we are able to track above 20 thousands objects in near-Earth space. In Figure 1 it is also visible we're already on exponential curve of growth of number of new satellites [38]. What is even worse, despite vastness of space, the object are placed on orbits which are convenient or preferable for a given kind of activity. By this, zones of heavy congestion are formed [39]. The described process increases the catastrophic failure risks not only for regular LEO operations but also all mission that in order to be deployed in deeper space, have to pass through heavily congested and, debris filled, regions (refer to Figure 2). While Kessler syndrome was conceived as accidental phenomenon arising purely from orbital mechanics and statistics, it can be negatively augmented by malicious activity of competing space powers. Anti-satellite weapon tests have already contributed significantly to amounts of debris humanity has to deal with [40].

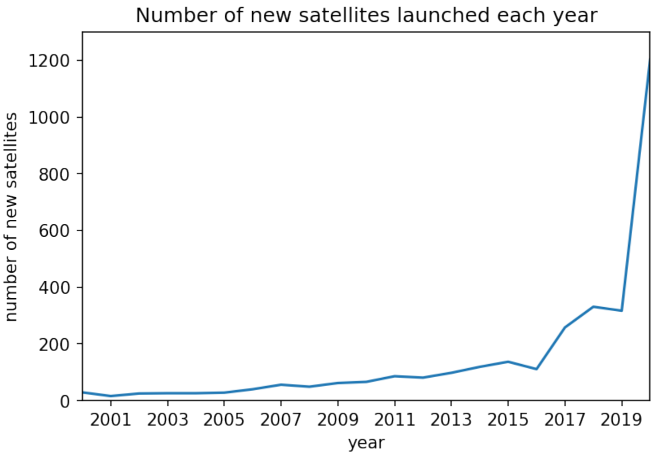

Fig. 1. Number of new satellites launched each years. Data source: [38]

What if collisions in space start becoming a result of intentional weaponization of the satellites?

H. Understanding the space domain

.

By now, it shall be apparent to the reader that systems of the space segment cannot be analyzed without taking into consideration the environment in which they operate. As famous Robert Hainlein is often quoted: "Once you're in orbit, you're halfway to anywhere". The reign of gravity can't be overcome, future satellite's positions can be only tweaked and will remain to large extent predictable. In space operations, counter-intuitively, physical closeness is not a measure of capability to link and physical separation is not a measure of capability to interact [42]. The physical environment, orbital considerations, Sun activity, the Earth's magnetosphere and the electromagnetic spectrum defines all space segment capabilities and limitations. The moment a satellite system is

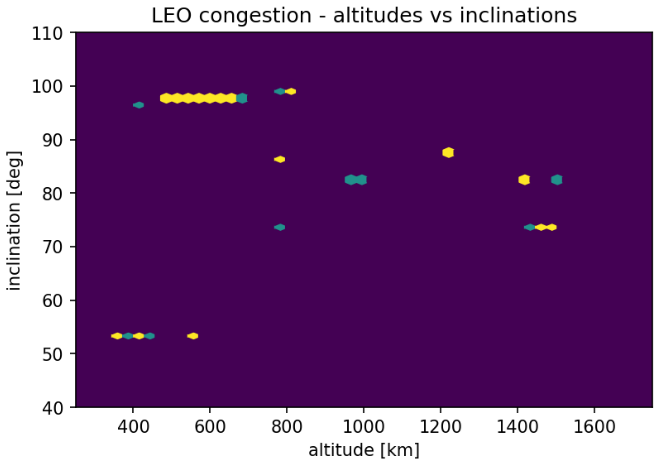

Fig. 2. Congestion zones in LEO. Data source: [41]

injected into its orbit and set up for operation, the margins for corrections and repairs have become very thin and are often limited to what the satellite provides in the first place. In particular after the end of the Space Shuttle area, human repair capabilities are severely limited and thus limited to robotic refurbishing missions. Consequently, all malfunctions that have not been taken into account during the design process, put the mission at risk. While the space engineering community has large appreciation for and prepares for tolerating accidental faults, there are still large gaps in understanding the full consequences of malicious behavior. Accidental faults follow well known statistics. In contrast, the drivers behind intentionally malicious faults, such as targeted attacks, remain the intention and incentives under which adversaries operate, not the statistics. The gap in understanding the threats to space systems and scale of societal and military dependence on space technologies and equipment, turns space into a critical infrastructure, which we analyze next in Section III.

III. SPACE IS A CRITICAL INFORMATION INFRASTRUCTURE

In Section I we have already seen that despite space infrastructure in itself not being a large business, large parts of our economic wealth and growth depend on it.

Global economy thrives thanks to safe and efficient navigation on the high seas provided by GNSS systems, with the help of AIS [43]. Aircraft, which move people and goods on large distances, also depend on uninterrupted GNSS system operations, supported by ADS-B reporting [44]. Oil rigs and pipelines, report the telemetry via communication satellites ensuring remote management of production [45]. Some mines are already using autonomous equipment which relies on both localization and communication capabilities provided from space [46].

If any of the the space dependent services becomes disrupted, chaos ensues. Without telemetry reports the whole production facilities have to stop to prevent infrastructure damage. All the vessels that require to be localized and navigated, have to stop to prevent crashes. It is not that there are no alternatives - they are, but it will take time to deploy them in the safe manner. The economy will stop for some time.

From the above example and the examples given in Section I, it is quite safe to write that most of our current and near future modern economy is in one way or another dependent on uninterrupted access to space as a conduit for information extraction and/or exchange. Crippling space infrastructure therefore means interfering with these sectors or, in less optimistic scenarios, disabling large parts of a country's economy (see Figure 3 for an overview of the dependence of individual economy segments). It should be noted that this dependence is particularly pronounced in developed countries, which justifies some of the adversary models we shall consider.

The danger of the current situation is that, both the degree of dependency nations have on space infrastructure and the depth of susceptibility of that infrastructure, are widely underestimated. Huge risks are looming from events (accidental or intentionally malicious ones) that may cripple a nation's access to space and thereby its economy and in part also its defense capabilities. Very little is done to increase the robustness and resilience of the space systems we rely on. The risk of a "Space Pearl Harbor" has been identified and announced as early as in 2001 and now applies to a majority of developed countries [47], [48].

This lack of resilience is partially caused by a phenomena called the "High Ground Fallacy", a concept originating from military doctrine of the old that armies would gain an advantage of being higher up and therefore unreachable by their enemy. Today, space is often called the new high ground, even in a civilian understanding of space systems. However, space assets are not the fortresses to seek shelter from the enemy or to descent on unprepared rivals. Instead, they are among the most fragile, remote, outposts that support main forces with information [42]. They are well reachable, both in the cyber-space and physically, as we shall see in the remainder of this survey. In particular, we shall see that they are reachable by entities insusceptible to the threats of space access denial or retaliation, which turns protecting space systems against advanced and persistent threats, the only viable option.

IV. A TAXONOMY OF SPACE THREATS

Space systems are exposed to a variety of threats and there are several ways to classify the latter. Previous analyses study threats to space systems from the perspective of international affairs, intelligence or military organizations, which tends to introduce bias of threats and countermeasures towards competing countries, namely other space powers. Threats investigated in that light are usually divided into two types: kinetic and non-kinetic, pertaining to type of energy exchanged between target and effector. An example threat classifications, which follows the above principle, is summed up below:

- **kinetic threats**
  - ground station physical attack [49]

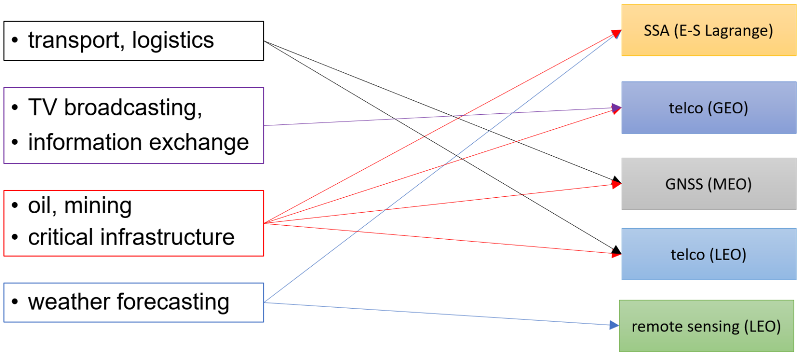

Fig. 3. Global economy segments dependency on space infrastructure

  - direct ascent anti-satellite weapons [49]
  - co-orbital attack system, capable of launching projectiles [49]
  - collision with other satellites (both active and defunct), debris, upper stages
- **non-kinetic threats**
  - high altitude nuclear detonation [49]
  - high-energy directed weapons [49]
    - lasers [49]
    - microwaves [49]
  - electronic
    - uplink jamming [49]
    - downlink jamming [49]
    - spoofing [49]
  - cyber
    - data intercept / monitoring [49]
    - data corruption [49]
    - seizure of control [49]

Threat classifications like the above, mainly due to the interests and focus of the organizations that published them, discuss threats in relation to global space powers (USA, Russia, China, India, perhaps, Japan, France, Israel, for some, also Iran and North Korea,) that may implement them (compare for example [7], [50], [51], [6], [49], [52]). The assumption is that exercising these threats requires capabilities of limited availability (typically only to nation states), including sophisticated launcher technologies, state-of-the art navigation and tracking (for kinetic attacks, but also, for ground based laser attacks or co-orbital microwave attacks), robotic rendezvous and proximity technologies (for orbital operations like the deployment of inspector spacecrafts with intended missions such as refueling, maintenance or operational life extension, covering activities up to Geostationary Orbits, but which can also be diverted from such objectives to bring down space vehicles), and outstanding, close and far range GNSS signal technology (e.g., for spoofing attacks). Table II summarizes most notable nation-state space powers and their counterspace capabilities, while [6], [49], [52] provide more detailed explanations and examples.

It is understandable that most of the community attention will be drawn to spectacular weapons, capable of tracking and physically destroying or, at least, damaging space systems. As mentioned before, there is not much that can be done about preventing or avoiding such attempts or outmaneuvering them. Yet, thankfully, we don't see many of such events, which as of to date are limited to technology demonstrations and targeted only to a nation's own vehicles.

There are several reasons for that: First, successfully intercepting or damaging a rival's orbital vehicle is considered an attack to that rival's territory. Space faring nations have established a balance of powers agreement, threatening retaliation, including between the two large defensive packs, in case space vehicles are attacked. The aggressor must therefore expect retaliation on earth, which might well ignite a spiral of uncontrollable escalation between the parties.

Second, physically destroying a vehicle multiplies the debris that must be tracked and avoided because it would otherwise destroy further space adding even more debris. The ultima-ratio of this effect is, introduced in II-G, Kessler's syndrome and will render space unusable for generations to come, cutting technologically advanced space-faring nations from the military and civilian applications that space provides.

Third, but of minor importance due to weak enforcement mechanisms, international space treaties would be violated that aim at regulating a safe, secure and sustainable use of this domain.

In developed countries, there is no real interest in actually risking the destruction of one's own infrastructure by clouds of debris or even preventing future use of such orbits for decades or until clean-up technologies become available. The kinetic hit to kill philosophy in space is clearly a double edged sword. In fact, weapons enabling near-space existential threats work in a way like nuclear weapons — they are capable of affecting everyone including those who yield them. In a similar fashion, like nuclear warfare, Mutually Assured Destruction worked so far to stabilize and build the balance between powers (however not making the world a better place). The risk of rendering near-space unusable has a chance to push the space powers

TABLE II
MOST-NOTABLE TECHNOLOGY EXAMPLES WITH ANTI-SATELLITE CAPABILITY

Technology	Examples
direct ascent vehicle	*Prithvi Delivery Vehicle Mark-II*, tested successfully in 2019,creating limited amount of debris [53] *Operation Burned Frost*, removal of defunct satellite conducted by SM-3 vehicle [54] Taking down of *Fēngyún 1C* defunct satellite by *SC-19* intercept vehicle [55]
co-orbital vehicle	*X-37B* USAF unmanned spaceplane [12] *Chongfu Shiyong Shiyan Hangtian Qi* reusable test spacecraft [13] *Aolong-1* active debris remove vehicle [56] *Kosmos 2519, 2521, 2523* small interceptor satellites performing randez-vous and proximity demonstrations [57] *Kosmos 2543* deployed *Kosmos 2542*, which in turn started to spy on U.S National Reconnaissance Office's US245 (with the NRO satellite performing maneuvers to steer off the adversarial inspector) [58] *SJ-17* experimental satellite performed very close proximity operations on dead and operating Chinese geostationary satellites, showing capabilities for both peaceful and hostile actions [59]
projectile deployment	*BX-1* deployment from *Shehzhou-7* mothership and *ISS* pass within 25 km (seemingly out of control) [60]
high altitude nuclear detonation	*Starfish Prime* was a nuclear explosion conducted at altitude 400 km, creating both electromagnetic pulse and artificial radiation belts. At least 6 satellite failures, that occurred in months that followed, are attributed to this experiment [61]
high energy directed weapons	operational laser systems like *Peresvet* [62] or *Sokol Eshelon* [63]. The latter is an origin of successful (but temporary) blinding of Japanese Earth observing satellite AJISAI [64]
communication eavesdropping	*Olymp-K / Luch* has been launched in 2014, as communication satellite. However, instead of maintaining its position and performing typical operations, it started to wander around GEO belt. As of 2020 it has shifted its position about 19 times [49], targeting mainly communication satellites, both military and commercially operated. Both, traversing of the GEO belt and close proximity operations sparked accusations of espionage and hostility (communication eavesdropping, inspection) [65], [66], [67].

rivalry into domains of non-existential threats.

The peaceful utilization of outer space is also a concern of the United Nations (UN), creating the UN Institute for Disarmament Research (UNIDIR) for monitoring and classifying all aspects related to international security and to assist in disarmament processes. UNIDIR hast spent more than 40 years evaluating technology development and tracking global activity in the context of space militarization. The Prevention of an Arms Race in Outer Space (PAROS) program was very successful in increasing and widely spreading awareness of threats and risks associated with placing weapons in orbit, much less in preventing space powers in exercising their space access and utilizing their denial capabilities [51].

However, space powers and, as we shall see, also non-space powers, less developed countries or even terrorist groups do not need to target space systems in a direct kinetic manner. Cyber- and electronic warfare allow for significantly more subtle, but still highly effective attacks that are much harder to attribute [50] and that require significantly less advanced equipment. If the the careful reader reviews the threat summaries referenced in this chapter, she will realize that majority of those surveys do not capture the vast possibilities of cyber or electronic attack on space infrastructure, which contributes to serious underestimation of, probability and the criticality of such event. Hacking a satellite grants adversaries control over the payload system and the applications it supports. Through it, they may spoof GNSS signals, disrupt, redirect, or manipulate communication, or use on-board systems for espionage. Hacking into the platform system or, for that matter, into a satellite's controlling ground station, grants full control over the satellite, including its orbit and mass. The latter two turn satellites into projectiles and kinetic weapons. The equipment required to reach satellites in orbit is relatively simple and, in particular, does not require capabilities of deploying or maintaining vehicles in space. An immediate conclusion from the last two aspects is obviously that threats of causing physical damage and ultimately Kessler's syndrome are not limited to developed countries, but also to countries and organizations that may not be as dependent on space or that may even benefit from the inaccessibility of this domain. In particular this includes asymmetric threats, which are naturally immune to the threat of Mutually Assured Destruction. Very few trusted and, proven to be effective, countermeasures exist against cyber and electronic attacks, especially when compared to kinetic domain (see Table 2 in [68]). It is not that the adequate countermeasure cannot be conceived. The problem lies in, perception of the threats, which we aim to change.

V. CYBER-PHYSICAL THREATS TO SPACE SYSTEMS

Spacecraft, space probes and space vehicles are cyber-physical systems: Satellites operate remotely, either alone or, to an increasing extent, in networked groups, but always in contact with ground stations, leveraging algorithms on their computer systems to control actuators, propulsion and sensors in order to fulfill their missions. As such they can fall prey to all threats more traditional cyber-physical systems (CPS) are exposed to, in addition to those originating from the harsh environment in which they operate and those relayed from the ground stations they communicate with. Concerns include classical security and dependability questions, like the confidentiality and integrity of sampled or relayed data, or the availability of subsystems, but also more specific ones, like misuse of the vehicle, including as a projectile or impactor [69].

In the following, we analyze the threat vectors spacecraft and space infrastructure are exposed to, the agents that exploit them and give examples of threats at various stages of the mission. Fig. 4) gives an overview of the units involved in deploying and operating spacecraft, which may be compromised by adversaries and exploited for attacking other units [70].

A. Terms and definitions

Threat vectors describe possibilities through which agents may gain access to system assets or resources [70]. A threat, as defined in the seminal work of Singer [71], is a product of the estimated capabilities of malicious actors and their intent. To defend a spacecraft against them, as many threats as possible need to be identified and evaluated against the abilities of potential malicious actors. Known weaknesses must be fixed, but since both identification and patching remain incomplete processes, spacecraft and supporting infrastructure should ideally also be prepared to tolerate threats, such as partially successful attacks, and return to a state at least as secure as initially. In other words, they must be resilient to accidental and intentionally malicious faults.

A *vulnerability* is a weakness or flaw in the system, its configuration or operation, that might be exploited when reachable by adversaries to gain an advantage over the systems and ultimately compromise it [70].

Exploited vulnerabilities lead to *faults* in the system, which may manifest in errors and ultimately lead to failure of the system [72]. We distinguish accidental from intentionally malicious faults. Whereas the natural processes that cause the former, the probability distributions they follow and their low-level effects are well understood, this is not the case for the latter. Whether, when and how frequent intentionally malicious attacks can be mounted are often just a question of the power an adversary can muster and of the incentives it has. Some adversaries operate with the resources of nation states, directly provided to them.

The situation is further complicated by a vast variety of weaponized software being available for analysis, re-purposing and deploying on the adversary-owned systems, but more importantly on systems of innocent users that have been compromised.

The proliferation of commoditized, low-cost space platforms, with almost no trade restrictions, common architectures and COTS technologies foreseen for NewSpace amplify this situation and expands the window of vulnerability for attacks [73].

B. Agents

The agents opposing space systems include governmental, military or commercial actors, but also individuals or organizations that undertake attempts to explore selected threat vectors. Since space systems require multidisciplinary knowledge and the equipment and software comprising such systems used to be rather rare and not easily obtainable, it was possible to exclude the occasional hacker from this list of adversaries. Other than that, the full spectrum of adversaries has to be expected [74], [75]:

- sophisticated individuals
- insiders / untrustworthy or careless personnel
- competitors / dishonest or careless business partners
- hacktivists
- criminal organizations / guerrillas
- nation states
  - state backed organizations
  - intelligence
  - military

Before analyzing the threats in further detail to which space systems are exposed, let us review the evidence we have from existing attacks, evaluated in section VI.

VI. REVIEW OF KNOWN ATTACKS

A. ROSAT failure

The earliest mention of counter satellite activity can be traced back to 1998 when ROSAT failed. ROSAT was an American-English-German scientific satellite that first experienced a malfunctioning reaction wheel used for attitude determination and, as a consequence, turned its instruments directly towards sun which destroyed it [76]. The ROSAT platform was plagued by faults and issues from its early days on [118]. The possibility that hackers might be responsible was raised a decade later by T. Talleur [77] in a confidential report along with a report on other malicious activities in the NASA networks. While, at the present moment, the original article is no longer available on-line (including in the Internet Archive), and the report is not publicly available for obvious reasons, the event has been reported by respected security researchers [119] and US security NGOs [120]. Currently the article is backed up on the author's blog [121].

Since there is no direct evidence for the malicious activity to be the root cause of final failure of ROSAT and not one of the existing other other plausible root causes, this incident has to be taken with a grain of salt.

B. Skynet

As reported by Reuters and Time [78], in February 1999, one of United Kingdom's Ministry of Defence military telecommunication satellites unexpectedly changed its orientation. Soon after, as the initial story goes, the MoD received a ransom request to gain back control over a critical piece of infrastructure. Early March that year, all allegations of a satellite hack and subsequent service interruption were denied by officials [79] and, in the end, ridiculed [122]. Whatever really happened then, the event sparked panic among military and intelligence personnel, to the extent that some (mis)information leaked to the public. If such an event actually took place, it would be evidence of the significant technical sophistication of an adversary or of a significant security misconduct on the defending side [123]. It is not very probable, but in the light of other, better documented cases, also potentially feasible.

TABLE III

SUMMARY OF PUBLICLY KNOWN SPACE INFRASTRUCTURE SECURITY INCIDENTS [5], [6], [7]

Year	Incident	Remarks
1998	ROSAT	Scientific satellite payload permanent failure coincidental with cyber-intrusion to mission control center, incident report classified [76], [77]
1999	Skynet	British military communication satellite allegedly taken over and ransom requested, lack of solid, public, evidence of incident [78], [79]
2000	GPS jamming during military trials	British and US tank had navigation problems during Greek trials. GPS jammers deployed by French security [80]
2003	Ames Research supercomputer shut down to halt intrusion	Swedish national persecuted, estimated costs > 1MUSD [81]
2003	TELSTAR-12 uplink jamming	TELSTAR-12 uplink was jammed, by source located in Cuba, during Operation Iraqi Freedom to prevent Voice of America broadcast over Iran [82]
2005	Sri Lankan rebels hijack satellite communications	Liberation Tigers of Tamil Eelam broadcast pirated TV & radio services to several countries [**?**]
2006	Data breach and multiple intrusions	NASA forced to block emails, Shuttle operations plans leaked [83], [84]
2007	Landsat-7	First unauthorized attempt to access the space segment [85], [86]
2008	Landsat-7 & Terrasat EOS interference	Very well documented hack attempt, large sophistication of adversary [85], [86]
2008	Worm infecting laptops on ISS	Brought by a Russian astronaut on Windows XP laptop. Malware quickly spread among other computers (although mission-critical equipment was safe) [87], [88]
2009	JPL data breach and malware spreading in NASA mission networks	Theft of 22GB of export-restricted data; thousands of connection set to external networks [89]
2009	BBC broadcast in Farsi disrupted	Telecommunication satellite jammed [90]
2009	NASA Goddard Center information leaked	Paid Earth imagery datasets posted online for free [81]
2010	GPS jamming by N. Korea	Multiple locations affected in S. Korea including Incheon International Airport. Aircraft had to rely on alternative navigation instruments. Incidents repeated couple of times in following years [91]
2010	NASA intrusions	Data destroyed or access restricted, 0.5 MUSD damage to Atmospheric Infrared Sounder (AIRS) program [92]
2011	NASA JPL breach	Hackers gained full access to JPL systems [93], [92]
2011	European communication satellite jamming	Deutsche Welle jammed on DeHotbird 8 satellite [94]
2011	NASA ISS command and control data leak	An un-encrypted NASA laptop was stolen. It contained the command sets, as well as, control algorithms for ISS [95], [92]
2011	JAXA H-2A Transfer Vehicle design leak	Virus infected laptop containing critical data [96]
2012	NASA and ESA identity and authentication data hacked and published	Around one thousand employees personal information leaked and posted in internet [97]
2012	JAXA Epsilon rocket design leak	Virus infected laptop containing critical data [98]
2014	DLR breach and data theft	Targeted malware found across DLR computers. Theft linked to China APT groups [99]
2014	Mulitple channels broadcast disrupted over Ethiopia	Arabsat telecommunication satellite jammed [100]
2014	NOAA satellite weather imagery service disrupted	Data flow from satellites affected by hack attributed to Chinese APT, systems forced offline [101], [102]
2015	*Turla* satellite communication links hijacks	*Turla* hacker group with links to FSB - hijacking internet services of older commercial satellites [103], [104], [105]
2015	*APT28* hacked French TV5Monde television	A professional, coordinated attack that disabled the TV broadcaster for couple of hours. It took months to fully replace destroyed equipment and return to regular operations [106]
2018	JPL intrusion	500 MB of critical documents leaked, unauthorized access to deep space network, operations affected for many months, [107], [108]
2018	malware in ISRO launch segment	suspected, ISRO named it false positive [109], [110], [111]
2018	DoD contractors hacked	Security breach with the possibility to exercise the control over satellite by hackers, data traffic disruptions. Additionally confidential design data on submarines and high fidelity satellite imagery stolen [112], [113]
2019	Advanced GPS signal spoofing in China	Ships GPS positions, reported by maritime satellite AIS system [114], [49]
2019	Successful attack on autonomous car navigation by GPS spoofing	[115]
2020	Worldwide advanced GPS signal spoofing	Ships located physically in waters near Norway, Libya, Malaysia, and Russia reported via AIS to sailing in circles off the San Francisco coast[116], [117]

C. Landsat and Terrasat EOS

Turning to better documented incidents, in late 2007 and 2008 two US government remote sensing, Earth observation satellites became subject to adversarial activity of unattributed origin (with presumptive evidence leading to a global competitor). In October 2007, Landsat-7 experienced about 12 minutes of interference, which was only discovered following the analysis of a subsequent event 9 months later. This second attempt to take over control over satellite was also not successful. In June 2008, Terra EOS AM–1, became subject to about 2 minutes of interference. The adversary, managed to complete all steps required for obtaining command authority over the satellite but refrained from issuing rogue commands. Four months later, the same satellite experienced a 9 minute hostile take over attempt, with all the steps required to take over control completed and again attackers restraining themselves from issuing rogue commands. Those events, clearly show the scale of threat and sophistication, as well as, the fact that malicious actors possess advanced knowledge on system operation details. Unlike the previous examples, the above events are credibly documented by Economic and Security Review Commission reporting to U.S. Congress [85], [86].

D. NASA JPL breaches

In November 2011, NASA's Jet Propulsion Lab discovered compromised accounts of several highly privileged users. The hackers had full systems access, enabling them to copy, modify and delete files as well as to create new user accounts. They could as well have uploaded malware for further exploitation of the NASA networks [93]. In the course of the investigation it was revealed that for the past 2 years, NASA was subject to significant adversarial activity, aiming at accessing the internal data networks, causing, both IP leaks and interruption of operations [92]. Unfortunately, the recommended strengthening of NASA JPL's defense posture was insufficient, as information that surfaced in June 2019 indicated another heavy network security breach, that happened in the Agency's flagship laboratory, 14 months earlier. This time an unauthorized Raspberry Pi microcomputer was found plugged into the facility network, providing cyber-access for adversarial activity, including access to confidential documentation and to the Deep Space Network (DSN) - an array of radio-telescopes used for ranging, telemetry acquisition and remote control of exploration probes traversing the Solar System. The scale of that compromise shall be alarming, as officials admitted, the hackers gained access to the gateway enabling them to take over or at least affect the mission control centers, including to those related to the human spaceflight program [107]. Malicious activity went undetected for 10 months. Initial damage assessment mentioned a leak of 500 MB of highly sensitive information, some under ITAR restrictions, and vast, long lasting disruption of network operation, including DSN and connections to other NASA sites [108].

E. NOAA

In October 2014, the flow of meteorological data from satellites operated by U.S. National Oceanic and Atmospheric Administration has been temporarily disrupted by an internet-sourced attack. Some forecasting services were disrupted, while the systems were under an unscheduled maintenance [101]. The incident analysis report stated that the organization did not sufficiently implement security requirements despite several audits that expressed this obligation. This lack of protection, left critical communication systems vulnerable, namely the satellite data feed and interfaces to other parts of critical infrastructure, including military [102].

F. Indian launch site malware infection

In December 2017, a malware *XtremeRAT* has been found by Indian and French independent researchers in India's Space Research Organization (ISRO) Telemetry, Tracking and Command Networks (ISTRAC) used for control and support of launch activities from the launcher ignition up to payload orbital injection. The malware could even have been present on a computer that was directly involved in launch operations [109]. *XtremeRAT* is a standard and widely available offensive tool used for accessing and taking control over a victim's system, often targeting critical infrastructure [110]. ISRO, after conducting an internal investigation, declared the incident as a false positive. The organization pointed to the fact that ISTRAC mission critical systems are air-gapped and thus secure against this type of adversarial activity [111]. Air gapping disconnects a computer from all external networks. History has shown that this approach is a challenge for hackers, but the one that can be, eventually, and, spectacularly, beaten as in famous *Stuxnet* malware [124]. However, having to maintain wireless connection to space vehicles, air-gapping space systems naturally remains incomplete, as the, reverse, space-to-ground infection path feasibility shall be also considered.

G. GPS spoofing

There is a significant number of cases where GPS signals have been either jammed or spoofed, a fact which is not very surprising given how weak those signals are when received on the ground, easing malicious interference. It is also not very surprising that adversaries have an incentive to mount such attacks, given how large the dependence of our society, economy and military on satellite navigation systems is. The GNSS receiver market is more than 97 BUSD worldwide, which is about one quarter of the global space economy in 2019 [1]. GNSS signals have been subject of extensive testing against jamming, meaconing or spoofing techniques for couple of years already [125]), however, today's receivers are still extremely easy to be tricked into false position, velocity and time reporting. *GPS crop circles phenomena*, sign of advanced GPS spoofing technology, has been first recorded in 2019 in several spots in China. As data received through the satellite Automated Identification System (AIS,[20]) indicate, ships that entered the spoofing area reported their positions as sailing in circles around arbitrary locations on land [114], [49]. In the following year, similar incidents happened on a worldwide scale, where a couple of ships around the world have been tricked into recognizing (and further, reporting through their AIS) its position off the coast of San Francisco [116], [117]. It is worth mentioning, that GPS spoofing is not only limited to close proximity of interfering equipment. Using relatively cheap and widespread technology (e.g., Software Defined Radio and open source software stacks [126], [127]) spoofing ranges of up to tens of kilometers can be achieved [128]. Using a large number of jamming devices, areas of the size of entire countries can be equipped with counter-GNSS technology [129]. In the near future, with more advanced technical deployments, like *Ekipazh* nuclear powered in-orbit electronic warfare satellites [130], [49], GNSS signal jamming or spoofing (or communication links disruption) could possibly affect much larger areas.

H. *Communication links hacks: Turla and APT28*

Since a significant part of existing space telecommunication infrastructure is based on analogue relays (*bent-pipe* concept) it is easy to jam inputs of such satellites. Essentially, all the adversary needs is to know the uplink frequency (which is public information) and a strong, directional source of interference. Unless, more complex, digital, regenerative payloads, are used, the only countermeasure to this attack is to track down the sources of interference and shut them down physically. There are cases were satellite communication infrastructure has been either target or conduit of more sophisticated attacks. In 2015 a *Turla* group has started a large-scale hijacking of satellite internet links in order to disguise their activity and hide their physical presence (since end-user terminals can be placed anywhere within the satellite service beam). Some of this activity was simply purchasing bidirectional links as any customer would do. However, to avoid the significant cost involved with this, *Turla* started to spoof packets of DVB-S based Internet system users. It was easy, because unlike its successor DVB-S2, DVB-S is not encrypted [103], [104], [105]. The same year, TV5Monde experienced a devastating cyberattack on a few of its broadcast facilities by hacker group *APT28*. The service (all 12 channels) was down for a couple of hours. It may not sound much, but broadcasters have contract obligations on signal availability and contract cancellation could jeopardize the company's existence. The attack was sophisticated and well prepared. Months earlier adversaries mapped TV5Monde networks, understanding how the broadcast process works and what equipment is involved. For grand finale, a malicious software was deployed, targeting critical broadcast devices and causing permanent hardware damage [106].

VII. THREAT VECTORS

In the following subsections, we now analyze systematically the threats to which space systems (see Fig 4) are exposed to in the individual phases of their lifecycle. We distinguish physical from cyber attacks, but highlight also where cyber attacks influence the physical world. We investigate to which extent a successful manifestation of these threats affect confidentiality or integrity of data, or, the availability of the spacecraft itself, before we provide in Section VIII a general scheme for the cyber-physical attacks on the space systems.

A. *Early phase attacks*

Before space infrastructure is even built and deployed in space, it undergoes long process of design, modification, assembly, integration and extensive testing. This is almost always a collaborative effort, involving many parties bringing different expertise, know-how and facilities. Hence, a large attack surface must be expected. It is also very important that as a single security compromise at those early stages, can not only stop or delay the program, but it may embed vulnerabilities that lay the foundation for later, more elaborate attacks on the developed ground or space system.

Attack vectors in this early phase affect satellite system design and development houses, component supply chains — D&D in Fig 4 —, assembly (manufacturing of mechanisms, electronic circuits), integration (assembling whole platform, payload, satellites), verification and validation (conducting the functional and environmental tests on integrated equipment) — AIVV in Fig 4. Vulnerabilities embedded at this stage may remain in existence well beyond the time when the satellite is finished, deployed into orbit and operated there.

At the early stage of system development, supply chain attacks offer a first interesting opportunity for adversaries to learn about the systems' capabilities. Moreover, state-backed agents may inject trojan-horses and other malware, both, at software and at hardware level, which constitutes an invaluable opportunity for further compromise of units after they become operational.

If the supply chain is of military grade, such attacks are not trivial, but still possible [134]. If the supply chain includes open source designs and components, as it is increasingly popular New Space ([135], [136], [137], [138], [139]), tainting of the design or its components seem easy at first glance, but are less trivial if they should both evade public analysis and the later validation process.

Similar activities, dealing mainly with documentation theft, unauthorized design alterations or simply deletion have to be expected at the integration stage. Some of the documents that are typically prepared in the course of developing satellite systems are more crucial than others. For example, Failure Modes, Effects and Criticality Analysis (FMECA) describe known failure modes and their assessment. It explains what is to be expected to go wrong and how the system is prepared to face the challenge. Such a document falling into the hands of adversaries informs them about the weakest link, which may guide them in the selection of the subsystem they target. More interesting even are the failure modes and effects which have evaded FMECA, as they pave the way for exploiting undocumented (and therefore likely untested) behaviors [133].

The test phase is another, very attractive epoch in the development life cycle to learn about or affect space systems. Knowledge about test procedures and methods for satellite system verification and validation, tells how a satellite system shall be utilized and which behavior is to be expected and which behavior constitutes anomalies. Adversaries could attempt to avoid exhibiting the latter to disguise their activity. Moreover, the test procedures themselves can be used to attack the space system, for instance by manipulating test equipment to leave critical functionality untested or by removing important steps from the procedure itself. It is also worth noting that failure of test equipment can destroy systems or delay their deployment. Even if the system under test is not destroyed, but pushed beyond the agreed range of operation, common procedure is that they have to be considered as broken and should not be deployed in space. The above threat vectors are

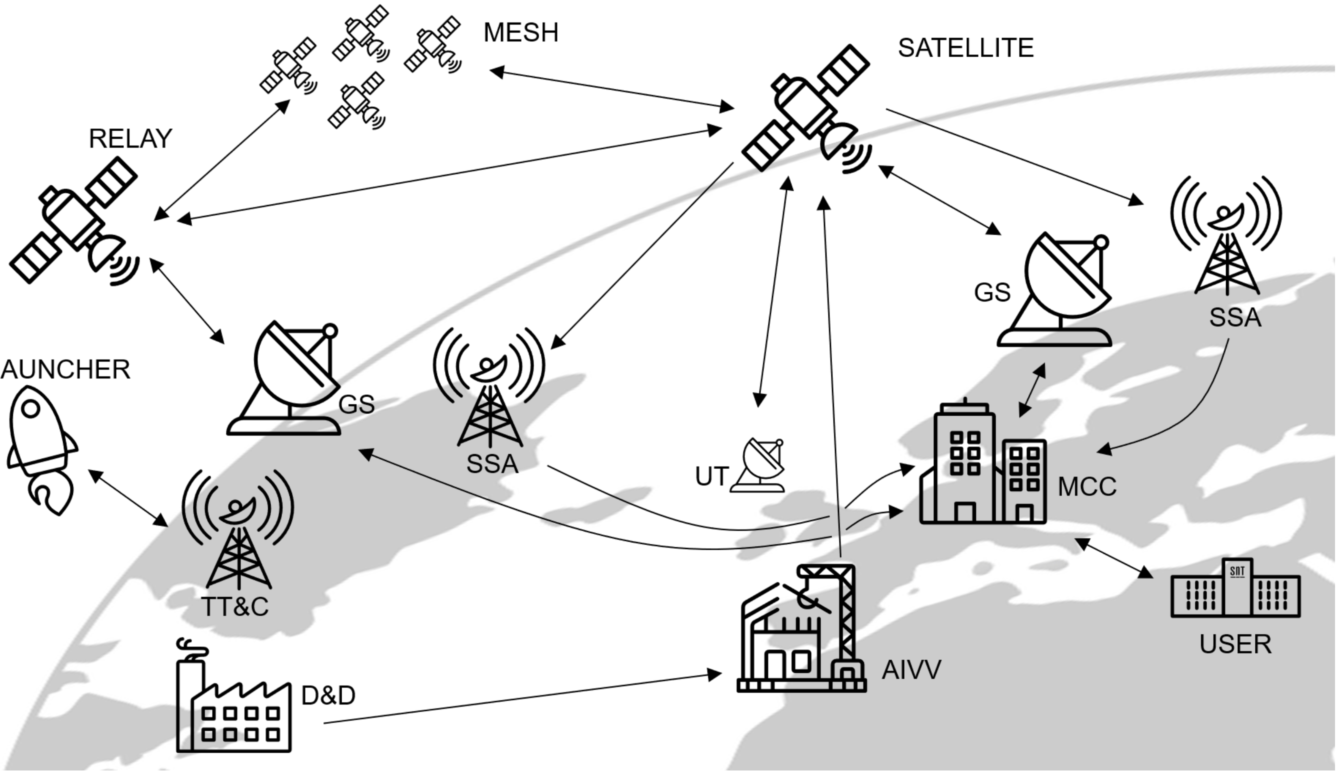

Fig. 4. Overview of space systems nodes

TABLE IV
CLASSIFICATION OF THREATS TO SPACE SYSTEMS - SUPPLY CHAIN, ASSEMBLY, INTEGRATION AND TESTS [75], [131], [132], [133], [49]

		Affecting		
		supply chain	assembly & integration	tests
loss of	confidentiality	design theft specification theft	documentation theft	test plan theft test results disclosure
	integrity	component tainting design modification	documentation modification	test specification modification test equipment settings modification
	availability	component supply disruption design deletion	documentation deletion integration facility unavailability	test equipment unavailability test results deletion

summed up in Table IV.

B. Ground segment attacks

The ground segment forms a large part of space infrastructure. Ground stations (GS on Fig 4) are responsible for communicating with space systems. Mission control centers (MCC in Fig 4) initiate and supervise the systems' operations and disseminate gathered data or provide other services to users (e.g., distribution of intelligence data, earth imaging or feeding in the broadcast signals from stations). The exact architecture of this segment will vary between systems but also depending on type of activity performed by the space systems. An important part of the ground segment is also the space traffic management or space situational awareness (SAA on Fig 4) infrastructure, which is comprised of ground facilities and responsible for tracking both, active and passive, space systems. Data processing centers archive and distribute ephemerids and conjecture assessment alerts to satellite system operators to warn about the risk of collision.

Ground stations are often considered choke points of the space system infrastructure [75], and are therefore most obvious and desirable targets of cyberattacks. Eavesdropping, at first, is useful for identifying the satellites a given facility communicates with. For ground stations this correlation is straight forward by means of which satellites the station can see. This is of course provided data is not relayed using satellites in this window to reach to other satellites.

For **mission control centers**, if linked with a distributed network of ground stations, more elaborate analysis is required. One needs to find out at least which ground stations are in the network. Breaking confidentiality at this stage helps

TABLE V
CLASSIFICATION OF THREATS TO SPACE SYSTEMS - GROUND SEGMENTS [75], [131], [132], [133], [49]

		Affecting			
		launch	ground station	mission control	space traffic management
loss of	confidentiality	payload disclosure tracking	eavesdropping tracking	eavesdropping (loss of encryption)	tracking
	integrity	trajectory modification GNSS meaconing / spoofing	masquerading message replay	modification of data modification of commands	man-in-the-middle attack tracked objects catalogue modification
	availability	loss of launcher no separation	denial of service jamming	denial of service facility unavailability	deletion of tracked objects catalogue observing station disablement

adversaries find out about physical (at GS i.e. RF signal encoding, framing) or higher lever (at MCC) communication protocols. Better prepared attackers can attempt to impersonate legitimate ground stations to communicate on their own or at least replay recorded communication. If attackers are able to masquerade as a mission control center (e.g., by stealing the center's authorization keys), they may modify or forge commands to obtain unconstrained access over a satellite system. As of today, satellites have no means to verify the sanity and safety consequences of received command streams. Hardest to mount would be attacks on GS or MCC availability, leading to the unavailability of the targeted facility. The spectrum of such attacks is very wide and spans from physical attacks to cyberattacks tempering with equipment in ground stations (antenna rotors, radome and rotor heaters, power outage). Cyberattacks on GS and MSS may deny the service of such stations and classical electronic warfare like RF jamming, saturating the station's receivers with locally produced emission, prevent reception or tracking of the satellite. Using directional RF beams, adversaries may even interfere with commands legitimately sent by a ground station.

Other, often overlooked, components of the ground segment that are however equally prone to attacks are the **space situational awareness** (SSA) facilities (laser and radar stations, telescopes) and the digital infrastructure (i.e. data centers) that support them. SSA serves (or will serve, as it is in an early stage of development) as space traffic management backbone, granting active spacecrafts the ability to avoid collisions with other, active or defunct spacecraft and with debris. The criticality of such a service for the safety of orbital operations cannot be underestimated as every failure adds to the complexity of the task it fulfills.

Another, often overlooked threat vector are attacks on the **post-processing infrastructure** of data relayed from satellites. Mission Control Centers feed data from satellites to processing facilities or to intermediary data operators, which process, store and index data before disseminating the post-processed data to end-users. A multitude of interfaces, network links, and facilities are managed by third parties, offering a very large attack surface for targeting the data stream. Attacks include data theft, disclosure, modification, deletion or corruption of data or metadata (communicated or stored), but also denial of service attacks on the data storage itself [133].

Traffic information, satellite ephemerides or orbital conjunction alerts, are distributed to satellite systems operators where this data is used for orbital corrections and most importantly collision avoidance maneuvers. Many of those information exchange systems are still using solutions from the 1970's, like Two Line Element's sets (TLEs [140]). If, as it is often the case, ephemeris data is sourced from just one organization, this would give rise to man-in-the-middle type of attacks, fiddling with the TLEs provided to satellite infrastructure operators, in order to orchestrate unnecessary maneuvers, or worse, collisions. Such an endeavor does not require significant processing power nor sophisticated equipment [141], which turns this attack into a serious threat for space systems, in particular for terrorist organizations and less developed countries, in particular as it targets the limited resources satellites are deployed with.

This threat has already been identified by international organizations, such as CCSDS, addressing the extremely low security concerns of TLE messages by designing a modern standard for orbital information dissemination, better prepared to withstand confidentiality and integrity attacks [142], [143]). Similar effects can be achieved by, less sophisticated, unauthorized deletion of selected ephemerides or of critical collision alerts.

The threat vectors of this subsection are summarized in Table V.

C. Launch segment attacks

The launch segment comprises launch vehicles and tracking, telemetry and command facilities which oversee the launch process. Since the whole launch process is quite rapid, it will be quite difficult for adversaries to launch elaborate attacks against the launched vehicle.

Attacks aim at revealing the launched payload, such as the type of satellite and its capabilities, and the orbital injection parameters, which can later be confirmed with the help of tracking capabilities in the hands of the adversary. Since the launch vehicle guidance is autonomous, malicious trajectory manipulation would have to target on-board computers before launch, which will be difficult, though not impossible. Also the time-frame of the launch process makes attempts to attack the launch trajectory by spoofing the GNSS receivers rather unpractical, in particular because many on-board guidance systems anyway rely on internal, inertial measurement units. Interesting attack targeting the launch process, would be to masquerade as a legitimate ground facility in order to issue self-destruct or course change commands, or to masquerade as a launch vehicle telemetry unit to report anomalous readouts, tricking the launch safety officers into executing safety procedures, which often lead to the destruction of the vehicle. Perhaps, the simplest attacks on a launch systems are acts of sabotage leading to loss of the launcher or preventing stages or payload separation (such events happen as an accidental human error [144], [145]). In many cases, such attacks require physical access to the vehicle, but some can also be mounted as a result of a cyberattacks, manipulating on-board systems prior to the launch.

The described threat vectors are summarized in Table V.

D. Space segment attacks

As can be seen in Fig. 4, the space segment is comprised of satellites (which, as described in Sec. II-B, are traditionally divided into a platform and a payload part), some of which assume the role of relaying units, and of groups of interconnected satellites (constellations, formations, clusters). Probes and deep-space exploration equipment would also fall into the satellite category. The only difference is their the size, in particular of the antennas required to remain in contact to ground and the amount of power devoted to transmission for successfully communicating with earth.

Depending on the exact space system application the system's architecture will differ significantly. The range of architectural possibilities spans from one satellite, connected to one ground station, to constellations of satellites, comprised of hundreds if not thousands of nodes. Constellation nodes increasingly become capable of two-way communication with numerous ground-based user terminals, but also, of communicating (node-hopping) with other satellites within the constellation and of relaying information using inter-orbit communication links. They are supported by an extensive ground stations network, serving as an information exchange gateway but also assisting in constellation control and management purposes [146].

Breaking confidentiality in the course of an attack, regardless of whether the attack pertains to platform or payload data, would be the most common way of taking unauthorized advantage of a satellite. For example, in the telecommunication domain, since satellites are used to provide services to vast areas on Earth by means of relatively small terminals, eavesdropping (or even integrity attacks by tampering with messages) have a really low entry threshold [146]. In fact, many heavily proliferated systems, have none or very weak, low-level encryption and authentication mechanisms, like DVB-S, with significant, easily exploitable vulnerabilities [147]. The expectation is to provide security mechanisms at higher levels of protocols [148], but this requirement will have to fight it's way through countless trade-offs as terminal power consumption, processing capabilities and overall complexity will be affected by encryption.

On the platform side, a similar process takes place, but the vision of total loss or platform takeover motivates better precautions, at least among the concerned, military and governmental, as well as international organizations. Again, a lot of civilian, especially scientific systems utilize CCSDS protocols, ensuring standardization (and thereby availability of equipment) and interoperability between different stakeholders and mission participants. An overview of how data systems (usually used in civilian exploration probes or scientific or general purpose satellites) are organized can be found here [149]. For example, the Space Packet Protocol [150] and the Space Data Link Protocol [151] do not contain any security measures (such as authentication, confidentiality, or integrity ensuring mechanisms) unless they are combined with the Space Data Link Security Protocol [152], which is optional, although encouraged. Obviously, in light of the examples shown in section VI, one must also take into consideration that encryption and authentication keys can be stolen or that a vulnerability in the encryption algorithm, or its implementation, is found, as has happened recently with SSL [153]. In such circumstances, adversaries not only become capable of eavesdropping communication. They may also access the spacecraft's internals and, if the adversary is sufficiently knowledgeable (compare VII-A), issue unauthorized commands to take over the vehicle (e.g., by installing new encryption keys) or to inject faults. Such activities can result in satellite systems switching to safe mode (reducing their functionality to what is essential to survive, sometimes less) or loss of the system or part of it (e.g., when adversaries points an Earth-observing telescope to the Sun to permanently damage opto-electronic components). Either way, availability of the system will be severely compromised.

Unfortunately, a direct access to on-board systems of a satellite, is not required to severely compromise availability of space-based service, as evidenced by numerous examples of electromagnetic interference attacks, collected in Table III.

RF jamming for, i.e. positioning system availability denial requires unsophisticated transmitter, interfering at frequency of interest with legitimate signals, saturating GNSS receiver inputs and preventing correct reception of position. There are even works available showing the possibility of selective GNSS signal denial, providing similar results, but harder to detect [154].

Jamming the communication satellite uplink channels (used to receive the signal to be further broadcast) is feasible, requires high power transmitters with directional beams, but it also requires them to be positioned relatively close to operator's transmitters (to target the high gain lobe of the receiving antenna on the satellite). Jamming the downlink might be easier on technical side (no pointing required, omnidirectional antennas and high power source of interference signal is sufficient), but requires more jammers to cover area of interest. Optical observation satellite payloads can be temporarily disabled by using high energy lasers, in similar manner as radio links are jammed.

The future of near-space exploitation open up new ways of

TABLE VI
Classification of threats to space systems - space and user segments [75], [131], [132], [133], [49]

		Affecting			
		space: platform	space: payload	space: formations	user terminal
loss of	confidentiality	unauthorized access	unauthorized access	eavesdropping	eavesdropping tracking??
	integrity	unauthorized access and commanding fault induction	unauthorized access and commanding fault induction	masquerading	data modification beaconing and spoofing
	availability	jamming platform failure	jamming blinding	jamming denial of service	jamming service disruption

attacking the systems. The LEO megaconstellations, which are being effectively deployed at the time of writing this paper, assume that nodes in the network are heavily interconnected. Such set-up offers extra opportunities for malicious behavior including eavesdropping by means of co-orbital vehicles (or masquerading as a valid network node that can be used for message relay). More advanced attacker could attempt to forge or to modify the messages in relay process, or simply drop them at convenient moments [133]. While such possibility of inter-satellite misbehavior can't be precluded, it requires a lot of technical efforts and such high level of sophistication, so it is rather be implemented for highest criticality assess (most likely in GEO, military or governmental communication relays). On the other hand, despite still being on drawing boards, satellite 5G communication networks are already scrutinized as opening another venue of system abuse, through vastly proliferated IoT devices [155].

The vectors of attack presented above (and summed up in Table VI) require elaborate knowledge about space systems, their construction and operation. Then, if executed properly, attacks of the above kind may allow adversaries to take over control, temporarily or permanently compromise the availability of the spacecraft or even turn it into an instrument of their purpose.

VIII. Scenario for Cyber-Physical Threat to Space Systems

Outstanding in the presented threat classification, as well as, in provided body of evidence, for real attacks on space infrastructure, is the fact, that ground stations along with the mission control center(s), are critical choke points of the trust in, and reliance on, satellite systems correct operation.

Indeed, many malicious activities are enabled if attacks can be conducted through the ground segment. Of course, countermeasures are available, in particular, air-gapping ground stations and mission control. Such measures can only make work of attackers a bit more challenging, but, will not prevent them from setting up their own rogue infrastructure or creating of targeted malware aimed at ground and space segment, thrown over the air-gap.

The deep reconnaissance of ground-and spacebased operational technology, will be the basis of all the attacks. To mount space system attacks, adversaries have to start by acquiring knowledge about the hardware/software stack of the satellite. This knowledge may be obtained from the bill-of-materials, leaked system specifications, or theft of FMECA documentation. Careful analysis of open hardware, open software and documentation collected from NewSpace vendors will help building up the required understanding of the space systems' capabilities, its limits and intended way of operation. Investigation and review of software components will be useful, especially if open source code is used on-board or on ground systems of interest. Obtained code can be analyzed for vulnerabilities or can be used for opening the supply chain attack vector. At this stage it will be of great importance to find out about safe-modes and contingency procedures of investigated systems. Attackers shall be interested in looking for ways of inducing the safe-mode, to either affect the functionality of a system (in safe mode system ensuring their own survival will very likely less secure than in nominal modes) or to conceal the breach.

The 2nd tier of cyberphysical attack requires obtaining access to a ground station, either by establishing a rogue station or by gaining an unauthorized access to an existing one. The former requires perpetrators to have valid cryptographic keys, full knowledge of the protocol stack and equipment capable of acquiring and maintaining radio links to the satellite, while the latter requires them to have access to the ground facility and remain undetected for long enough to complete their attack. With the advent of heavily distributed, Ground Station as a Service ventures this path becomes easier, as the more stakeholders mean more chances of some party not conforming to security regulations. On the other hands, similar effect could be achieved by tinkering with user terminals, especially if are mass produced for Internet of Things, but many examples show that industrial grade VSAT can be easily compromised and provide unauthorized access to services.

Accessing the 3rd tier of cybyr-physical attack on space system involves tracking the space system and monitoring it's behavior. Tracking reveals when the satellite is in the communication windows with the compromised (or rogue) ground station and for how long this window will remain open. Information about the length of this visibility window is crucial for select short slots (that might not be used by operators) for test connections or to select the ones that are sufficiently long to finalize the attack on the space system in

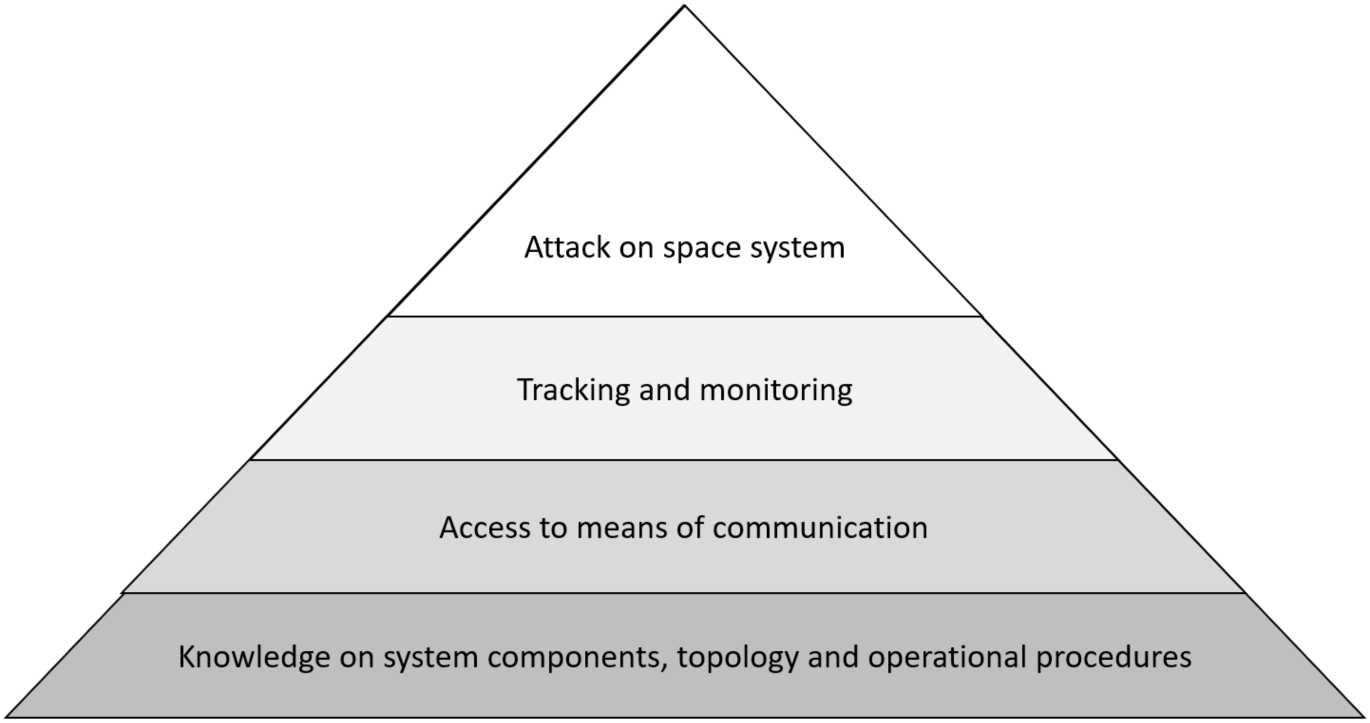

Fig. 5. Stages of space cyber-physical system attack

one attempt. Monitoring the system behavior requires reading out telemetry reports and keeping track of system power input, battery charge state, current loads, mode of operation, payload status, reaction wheel speeds, is required to know what type of attack is suitable and when the attack is most effective to damage the vehicle(e.g. by draining the batteries by switching on loads while in eclipse, changing attitude to burn optical payload by directing it to Sun, attempting to change the orbit by enabling the propulsion, switching to safe mode, if it is not safe to do so).

By satisfying the requirements of first three stages, adversaries will be well suited for conducing their attack successfully, taking control over the space vehicle and inflicting damage to the system, or by leading it to destroy itself or others.

One inherent weakness in today's operation of the space segment is that vehicles in the latter accept commands and tasks received from ground as fully trusted as long as they can decode these commands correctly. Sanity checks and more elaborate communication schemes that would prevent total system takeover in case a ground facility is compromised are rarely considered or applied.

Moreover, with the proliferation of standard hard- and software components, targeted exploits not only affect single spacecraft, but may bring down whole constellations of satellites. We already see this effect on ground based systems where homogeneity of automotive equipment bears a similar threat of adversaries taking ov'er entire fleets. In all that, satellites must be considered not only as digital assets but as cyber-physical systems with all involved threats, both to the satellite itself and to its environment if it gets under control of an adversary [133], [156].

While attacks on the user segment are "low hanging fruits" that can be relatively easily reaped benefit from, attacks on space segment require a more coordinated effort and substantial resources.

Figure 5 shows the subsequent stages on which an attacker has to focus to mount his/her space cyber-physical system attack.

IX. WHAT MUST CHANGE?

Certainly, we should not ignore the possibility of future targeted cyber attacks to space vehicles. However, unfortunately the solutions we apply to protect ICT systems on the ground, primarily following the arms race between new threats being revealed and patches trying to fix known vulnerabilities, only apply to a limited extent to space vehicles (and they have not be proven very effective in the past). We have to try to anticipate attacks, assume they will be partially successful and prepare the system for tolerating such attempts without already causing damage in order to buy the time for other mechanisms to return the space vehicle to a state at least as secure as before the attack.

In light of threats yet to reveal themselves over the multi-decade lifespan of many satellites, coupled with the virtually non-existent (as of the moment of writing) physical access and hardware upgrade capabilities to the satellites, once deployed, it will be essential to prepare upfront for any form of recovery that may have to be applied later.

A. Resources

Essentially the above strategy boils down to ensuring that sufficient resources will be available at all points in time to throw out adversaries or compensate for occurrence of complex, sometimes Byzantine faults, and return the system to security and, most importantly, safety for both, the vehicle and its environment. With care, these resources will be exclusively computation resources, needed to improve the software stack over time, but also to retain the degree of replication that is already available to ensure safety despite accidental faults.

The critical element of the above sentence is availability, in particular in the presence of targeted attacks. Loosing static trust anchors (e.g., because of compromised ciphers) will grant adversaries full control over the system (assuming that the telecommand channel has already been taken over by adversaries). On the other hand, when considering reconfigurable trust anchors, the same reconfiguration interface, required to build long-term security by continuously updating said trust anchor, presents itself, as an attractive opportunity for adversaries. This opportunity not only widens the satellites attack surface, but also gives them the opportunity to install a permanent foothold.

In the following, we review some of the resources of a space vehicle to derive guidance for future system architectures and their assurance processes.

B. Platform and Payload

As provided body of evidence shows, both platform and payload can be attacked in cyber and physical domains. They suffer from single point of failure syndromes, which despite deploying extensively redundant architectures nowadays, are inevitable (i.e. especially payloads are not expected be fully redundant). Today, the only known principle measures to mitigate single point of failure syndromes are the construction of components that cannot fail (a futile endeavor in highly radioactive environments and with systems of not trivial complexity) and the replication and distribution of functionality, so that not all replicas fail simultaneously. Replication may and shall happen at many levels: starting from components constituting the system, to the systems (crafts, vehicles) up to the system-of-systems (swarms, formations, constellations). However, replication is necessary but not sufficient to achieve the goal of unconditional fault mitigation. If the replicas do not cooperate actively to tolerate the failures or compromises, the dedicated attacker or unfortunate accidental fault will overcome the protections and posses the system. Hence, to further eliminate the residual risk of compromise and, in particular, of fault propagation, outcomes of replicated system shall be applied only after consensus on the outcome, has been reached. Consensus becomes the last line of defense (e.g., after plausibility checks have confirmed the validity of control signals), especially when interfacing to actuators or while accepting commands and appending the on-board schedule.

All that being said about replication, in space context, it is not an absolute remedy for all safety and security concerns, mainly due to power, mass, bandwidth and accessibility constraints that the space infrastructure exhibits. Therefore, we advocate further research in ways of accommodating consensus based replication, especially taking into account incoming technology improvements (efficient resource utilization) and proliferation of distributed space systems.

C. Ciphers

Ciphers securing data, but more importantly command streams, including the software or gateware updates and fixes are and will be required, we therefore have to anticipate that the cipher, its implementation or the used keys need update, possibly much more frequent than the remaining software stack itself. Some of these elements can be constructed from others (like session keys from a secret possessed and used to authenticate a node, and the latter being derived from a host key to limit how often this host key is exposed). However, the root algorithm itself and the key used to receive it in case all other levels are compromised, remain critical. To also replace this root of trust, sufficient resources must be provided to host future replacements of the root encryption algorithm, including sufficient memory to hold the new root key. Then the root key can be used to decrypt the received replacement, before the vulnerability can be exploited, if necessary proactively, in case the security of the root algorithm is at risk.

From this point onward, patches can be validated and installed, and the subsequent command sequence authenticated and applied.

D. Communication

Communication links, both ground and space ends, are critical points of entry that deserve special attention. First, those subsystems are complex, thus inherently contain exploitable vulnerabilities and are exposed directly to adversaries, in such way we can't prevent their attempts to tinker with defended infrastructure.

In our opinion, the only viable solution can be found in replication mechanism extending into time and space domains. In time domain, it is outpacing adversaries in compromising the critical communication links needed to patch subsystems themselves if this enable bypassing the authentication and authorization mechanisms.. This implies frequent resets of these most critical communication systems, possibly in combination with replication to circle through just repaired entities, which the adversary would need to compromise again before she can continue with its attack. In space domain, replication means having mutually independent commanding paths (direct but also relayed through other networks and nodes), commanding centers (coordinating, among themselves, on the ground, the commanding actions and schedules) and on-board decoders capable of sharing collected inputs form mission controls and exercising the consensus algorithms on them. While such approach would improve the space infrastructure safety and security enormously, as of the moment of writing, it has not been implemented.

E. Processes and Assurance

Of course, for all elements where speed is of essence, in particular fixing vulnerabilities, existing validation and assurance processes are simply too slow to outpace adversaries in their doing. Pre-assured components may be a solution, but absolute confidentiality needs to be applied to ensure knowledge on how to attack them is not leaked to the adversary. A possibly better option would be to restrain components to the roles they have to play and live with the residual risk of patches introducing new vulnerabilities, which adversaries would still need to identify before they can be exploited. Then, with enough time outside the critical moments of the satellite being under attack, patches can be hardened to improve their correctness.

Restraining requires limiting access to resources to only those essential for the purpose of a component and may, as described for actuators as well benefit from replication and voted access to all configuration possibilities.

X. CONCLUSIONS

In this paper, we have surveyed existing and reported attacks to develop a comprehensive survey of threats space systems are exposed to. Unlike previous studies, the attacks we are most worried about include cyber attacks possibly mounted by small groups of hackers with relatively simple equipment or leveraging the compromised equipment of space-faring nations to take control over space vehicles with possibly severe consequences on the defense capabilities, but more importantly the economy of developed countries. Adversaries compromising GNSS may impact navigation, logistics and other businesses that depend on this service, and with satellite control in the hands of such groups, they may even turn the captured vehicle into a cyber-kinetic weapon, targeting other space craft or ultimately triggering Kessler's syndrome, which would render space inaccessible to developed nations for the upcoming decades until debris capture technology becomes available.

In our opinion, such asymmetric threats are best countered by leveraging on the already widely deployed accidental fault tolerance mechanisms to prepare satellites to also tolerate targeted attacks to buy the time required to rejuvenate them to a state at least as secure as initially. Clearly, such an effort requires significant changes, including of the assurance processed deployed for "Old Space", but more importantly also for "New Space" equipment, but also increased situational awareness and the will and resources (partially in space) to achieve this tolerance.

We can predict fault and mitigate risks accordingly, but some faults, even if obeying statistics might be Byzantine for which the systems might not be ready. Byzantine fault is accidental equivalent of malicious activities. It might be interesting not to focus on safety only, or on security only, but to focus on Byzantine fault models instead and building the systems with Byzantine fault tolerance.

In context of this paper it is interesting exercise to read about vision of futuristic counterspace activities as written by Zielinski et al. in the 90's [157] for 20th century. What's striking during this lecture is that many of the predictions became reality much sooner than anticipated (extreme miniaturization, satellite cloaking, ground based high energy lasers, proximity operations and satellite bodyguards, precise optical and radar tracking) later became a reality with the rest of the concepts quickly catching up. We believe, the same will happen to cyber-physical warfare in space - once implausible, unlikely, too expensive, not practical, in near future will become everyday reality of space exploration and exploitation.

REFERENCES

[1] "The 2019 global space economy at a glance," Available at https://brycetech.com/reports/report-documents/Bryce_2019_Global_Space_Economy.png (2020/10/13).

[2] "Gross domestic product data files," Available at https://data.worldbank.org/indicator/NY.GDP.MKTP.CD?year_high_desc=true (2021/04/21).

[3] "List of countries by GDP (nominal)," Available at https://en.wikipedia.org/wiki/List_of_countries_by_GDP_(nominal) (2021/04/21).

[4] R. Hollingham, "What would happen if all satellites stopped working?" Available at https://www.bbc.com/future/article/20130609-the-day-without-satellites (2021/04/21).

[5] J. Fritz, "Satellite hacking: A guide for the perplexed," in *Culture Mandala: Bulletin of the Centre for East-West Cultural and Eco-nomic Studies*, vol. 10, 2013.

[6] "Space scurity index," Available at https://www.spacesecurityindex.org (2020/10/14), Tech. Rep., 2019.

[7] M. Horovitz, M. Randles, and R. Levi, "Space cybersecurity's final frontier," Available at https://static1.squarespace.com/static/56d0212027d4bded627db544/t/56deb84c3c44d8eb68c68083/1457436755011/LCS+June+Report-web.pdf (2020/20/14), London, UK, Tech. Rep., Jun 2015.

[8] R. Reesman and J. R. Wilson, "The physics of space war: How orbital dynamics constrain space-to-space engagements," The Aerospace Corporation, Center for Space Policy and Strategy, Tech. Rep., Oct 2020. [Online]. Available: https://aerospace.org/paper/physics-space-war-how-orbital-dynamics-constrain-space-space-engagements

[9] D. A. Vallado, *Fundamentals of astrodynamics and applications*, 4th ed. Hawthorne: Microcosm Press, 2013.

[10] C. A. C. A. Kluever, *Space flight dynamics*, ser. Aerospace series (Chichester, England), 2018.

[11] G. Dekoulis, *Space Flight*. InTechOpen, 2018.

[12] M. Wall, "X-37B: The Air Force's mysterious space plane," Available at https://www.space.com/25275-x37b-space-plane.html (2021/02/15).

[13] S. Clark, "China tests experimental reusable spacecraft shrouded in mystery," Available at https://spaceflightnow.com/2020/09/08/china-completes-test-flight-of-experimental-reusable-spacecraft/ (2021/02/15).

[14] W. J. Larson and J. R. Wertz, *Space mission analysis and design*, ser. Space technology library 1666421. Torrance: Microcosm, 1992.

[15] J. R. Wertz, D. F. Everett, and J. J. Puschell, *Space mission engineering : the new SMAD*, ser. Space technology library v. 28. Hawthorne, CA: Microcosm Press Sold and distributed worldwide by Microcosm Astronautics Books, 2011.

[16] "International Space Station," Available at https://en.wikipedia.org/wiki/International_Space_Station (2021/09/01).

[17] "Voyager 1," Available at https://en.wikipedia.org/wiki/Voyager_1 (2021/09/01).

[18] "Very Small Aperture Terminal (VSAT)," Available at https://en.wikipedia.org/wiki/Very-small-aperture_terminal (2021/09/01).

[19] "Satellite Navigation Device," Available at https://en.wikipedia.org/wiki/Satellite_navigation_device (2021/09/01).

[20] "Automatic Identification System (AIS)," Available at https://en.wikipedia.org/wiki/Automatic_identification_system (2021/09/01).

[21] “Automatic Dependent Surveillance–Broadcast (ADS-B),” Available at https://en.wikipedia.org/wiki/Automatic_Dependent_Surveillance%E2%80%93Broadcast (2021/09/01).

[22] “Tiangong Space Station,” Available at https://en.wikipedia.org/wiki/Tiangong_space_station (2021/09/01).

[23] “Aremis program,” Available at https://www.nasa.gov/artemisprogram (2021/09/01).

[24] “Apollo program,” Available at https://en.wikipedia.org/wiki/Apollo_program (2021/09/01).

[25] “European Cooperation for Space Standardization,” Available at http://ecss.nl/standards/active-standards/ (2021/09/02).

[26] “NASA Technical Standards System,” Available at https://standards.nasa.gov/nasa-technical-standards (2021/09/02).

[27] “Let’s talk about NewSpace,” Available at https://blog.satsearch.co/2019-02-26-lets-talk-about-newspace (2021/09/02).

[28] “Tailored ECSS engineering standards for in-orbit demonstration cubesat projects,” Available at https://copernicus-masters.com/wp-content/uploads/2017/03/IOD_CubeSat_ECSS_Eng_Tailoring_Iss1_Rev3.pdf (2021/09/02).

[29] “Cubesat 101: Basic concepts and processes for first-time cubesat developers,” Available at https://www.nasa.gov/sites/default/files/atoms/files/nasa_csli_cubesat_101_508.pdf (2021/09/02).

[30] “Start-up space report 2021,” Available at https://brycetech.com/reports/report-documents/Bryce_Start_Up_Space_2021.pdf (2021/09/02).

[31] “Smallsats by the numbers, 2020,” Available at https://brycetech.com/reports/report-documents/Bryce_Smallsats_2020.pdf (2020/10/27).

[32] “State of the satellite industry report, 2021,” Available at https://brycetech.com/reports/report-documents/SIA_SSIR_2021.pdf (2021/09/02).

[33] D. J. Kessler and B. G. Cour-Palais, “Collision frequency of artificial satellites: The creation of a debris belt,” *Journal of Geophysical Research: Space Physics*, vol. 83, no. A6, pp. 2637–2646, 1978. [Online]. Available: https://agupubs.onlinelibrary.wiley.com/doi/abs/10.1029/JA083iA06p02637

[34] S. A. Jacklin, “Small-satellite mission failure rates,” Available at https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20190002705.pdf (2020/10/07), Moffett Field, CA, Tech. Rep., Mar 2019.

[35] M. Williams, “About 3Available at https://phys.org/news/2020-10-starlink-satellites.html (2021/09/02).

[36] “Megaconstellation,” Available at https://en.wikipedia.org/wiki/Satellite_internet_constellation (2021/09/02).

[37] “O3b mpower,” Available at https://en.wikipedia.org/wiki/O3b_mPOWER (2021/09/02).

[38] “UCS satellite database,” Available at https://www.ucsusa.org/resources/satellite-database (2021/09/03), Tech. Rep., May 2021.

[39] S. Lemmens and F. Letizia, “ESA’s annual space environment report,” Available at https://www.sdo.esoc.esa.int/environment_report/Space_Environment_Report_latest.pdf (2021/09/03), Tech. Rep., May 2021.

[40] “2007 chinese anti-satellite missile test,” Available at https://en.wikipedia.org/wiki/2007_Chinese_anti-satellite_missile_test (2021/09/03).

[41] “Bulk catalog for Low Earth Orbit,” Available at https://www.space-track.org (2021/09/03).

[42] J. E. Oberg, *Space Power Theory*, 1st ed. US Air Force Academy, 1999.

[43] “Marine Traffic - ship tracking and maritime intelligence,” Available at https://www.marinetraffic.com (2021/09/27).

[44] “Flight Radar - aircraft tracking,” Available at https://flightradar24.com/ (2021/09/27).

[45] R. G. Burke, “China satellite SJ-17, friendly wanderer?” Available at https://www.offshore-mag.com/business-briefs/article/16759406/satellite-communications-how-the-petroleum-industry-is-using-satellite-services (2021/09/27).

[46] “Autonomous haulage systems for mining industry: Leading manufacturers,” Available at https://www.mining-technology.com/mining-safety/autonomous-haulage-systems/ (2021/09/27).

[47] J.-M. Stoullig, “Rumsfeld commission warns against "space pearl harbor",” Available at https://www.spacedaily.com/news/bmdo-01b.html (2021/04/22).

[48] B. Spring, “U.S. national security policy toward space: The debate that should end but won’t,” Available at https://spacenews.com/us-national-security-policy-toward-space-debate-should-end-wont/ (2020/11/04).

[49] T. Harrison, K. Johnson, J. Moye, and M. Young, “Space threat assessment 2021,” Available at https://www.csis.org/analysis/space-threat-assessment-2021 (2020/04/28), Washington D.C., USA, Tech. Rep., Apr 2021.

[50] R. P. Rajagopalan, “Electronic and cyber warfare in outer space,” Available at https://unidir.org/publication/electronic-and-cyber-warfare-outer-space (2020/10/13), Tech. Rep., May 2019.

[51] B. Silverstein, D. Porras, and J. Borrie, “Alternative approaches and indicators for the prevention of an arms race in outer space,” Available at https://unidir.org/publication/alternative-approaches-and-indicators-prevention-arms-race-outer-space (2020/10/13), Tech. Rep., May 2020.

[52] B. Weeden and V. Samson, “Global counterspace capabilities, an open source assessment,” Available at https://swfound.org/media/207141/swf_global_counterspace_capabilities_2021.pdf (2021/04/01), Tech. Rep., Apr 2021.

[53] A. J. Tellis, “India’s ASAT test: An incomplete success,” Available at https://carnegieendowment.org/2019/04/15/india-s-asat-test-incomplete-success-pub-78884 (2021/04/21), 2019.

[54] P. J. Blount and J. I. Gabrynowicz, “USA-193: Selected document,” *The Journal of Space Law, A Supplement*, vol. 1, no. 1, 2009. [Online]. Available: https://airandspacelaw.olemiss.edu/pdfs/usa193-selected-documents.pdf

[55] M. C. Mineiro, “FY-1C and USA-193 ASAT intercepts: an assessment of legal obligations under article IX of the outer space treaty.” *Journal of Space Law*, vol. 34, no. 2, p. 356, 2008.

[56] K. Mizokami, “Is china’s space junk collector a weapon in disguise?” Available at https://www.popularmechanics.com/military/weapons/a21627/china-space-junk-collector-potential-weapon/ (2021/04/20).

[57] M. Wall, “’very abnormal’ russian satellite doesn’t seem so threatening, experts say,” Available at https://www.space.com/41511-weird-russian-satellite-not-so-abnormal.html (2021/04/20).

[58] L. Grush, “Russia just tested satellite-destroying tech in space, US Space Command claims,” Available at https://www.theverge.com/2020/7/23/21335506/russia-anti-satellite-weapon-test-kosmos-2543 (2021/04/20).

[59] C. CLark, “China satellite SJ-17, friendly wanderer?” Available at https://breakingdefense.com/2018/04/china-satellite-sj-17-friendly-wanderer/ (2021/04/20).

[60] B. Weeden, “China’s BX-1 microsatellite: a litmus test for space weaponization,” Available at https://thespacereview.com/article/1235/1 (2021/04/20).

[61] “Starfish prime,” Available at https://en.wikipedia.org/wiki/Starfish_Prime (2021/04/20).

[62] B. Hendrickx, “Peresvet: a russian mobile laser system to dazzle enemy satellites,” Available at https://www.thespacereview.com/article/3967/1 (2021/04/20).

[63] D. A. Day, “Hubble in the crosshairs,” Available at https://www.thespacereview.com/article/1865/1 (2021/04/20).

[64] “Sokol Eshelon,” Available at https://en.wikipedia.org/wiki/Sokol_Eshelon (2021/04/20).

[65] M. Gruss, “Russian luch satellite relocates — next to another intelsat craft,” Available at https://spacenews.com/russian-luch-satellite-relocates-next-to-another-intelsat-craft/ (2020/10/08).

[66] J. Leicester, S. Corbet, and A. Mehta, “’Espionage’: French defense head charges Russia of dangerous games in space,” Available at https://www.defensenews.com/space/2018/09/07/espionage-french-defense-head-charges-russia-of-dangerous-games-in-space/ (2020/10/08).

[67] P. Tran, “Foreign governments are approaching French satellites in orbit, says space commander,” Available at https://www.defensenews.com/space/2018/01/26/foreign-governments-are-approaching-french-satellites-in-orbit-says-space-commande (2020/10/14).

[68] T. Harrison, K. Johnson, and M. Young, “Defense against the dark arts in space: Protecting space systems from counterspace weapons,” Available at https://www.csis.org/analysis/defense-against-dark-arts-space-protecting-space-systems-counterspace-weapons (2021/04/02), Washington D.C., USA, Tech. Rep., Feb 2021.

[69] "Computer Security Resource Center Glossary: Cyber Threat," Available at https://csrc.nist.gov/glossary/term/Cyber_Threat (2021/03/25).

[70] "Vulnerabilities, threat vectors, and probability," Available at https://www.professormesser.com/security-plus/sy0-401/vulnerabilities-threat-vectors-and-probability/ (2021/03/10).

[71] J. D. Singer, "Threat-perception and the armament-tension dilemma," *The Journal of Conflict RSesolution*, vol. 2, no. 1, pp. 90–105, 1958.

[72] A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing," *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, 2004.

[73] T. Wrightson, *Advanced Persistent Threat Hacking*, 1st ed. McGraw-Hill, 2014.

[74] "Science and Technology, Cybersecurity, Insider Threat," Available at https://www.dhs.gov/science-and-technology/cybersecurity-insider-threat (2021/03/25).

[75] "Security threats against space missions," The Consultative Committee for Space Data Systems, Informational Report CCSDS-350-1-G-3, Apr 2020. [Online]. Available: https://ccsds.org

[76] K. Epstein and B. Elgin, "Network security breaches plague nasa," November 2008.

[77] T. J. Talleur, "Russian domain attacks against nasa network systems," Classified as "For Official Use Only—No Foreign Dissemination", Tech. Rep., January 1999.

[78] L. Grossmann, "Did hackers hijack a british military satellite?" Available at http://content.time.com/time/magazine/article/0,9171,20673,00.html (2020/10/07).

[79] "Satellite hack raises security questions," Available at https://www.cnet.com/news/satellite-hack-raises-security-questions/ (2020/10/07).

[80] L. Grau, "Gps signals jammed during tank trials," *Military Review*, vol. 81, no. 2, pp. 12–16, 2001.

[81] P. K. Martin, "Letter to senators answering questions on status of nasa cybersecurity incidents investigations," Available at https://oig.nasa.gov/audits/reports/FY12/Export_Control_Letter(1-25-12).pdf (2020/10/14).

[82] M. Corneau, "Unprecedented. space-based information in operation iraqi freedom," *Space Army Journal*, pp. 48–63, 2003.

[83] A. Boyle and J. Oberg, "Security conscious NASA tightens e-mail policy," Available at http://www.nbcnews.com/id/16095705/ns/technology_and_science-security/t/security-conscious-nasa-tightens-e-mail-policy/ (2020/10/15).

[84] "Hacker charged for breaching NASA computers," Available at https://www.newscientist.com/article/dn10723-hacker-charged-for-breaching-nasa-computers/ (2020/10/15).

[85] U. S.-C. Economic and S. R. Commission, "2011 annual report to congress, chapter 2, section 3: The implications of china's civil and military space activities," Available at https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf (2020/10/07), Tech. Rep., Nov 2011.

[86] ——, "2015 annual report to congress, chapter 2, section 2: China's space and counterspace programs," Available at https://www.uscc.gov/annual-report/2015-annual-report-congress (2020/10/07), Tech. Rep., Mar 2015.

[87] "Computer viruses make it to orbit," Available at http://news.bbc.co.uk/2/hi/technology/7583805.stm (2020/10/15).

[88] M. Moore, "Computer virus infects international space station laptops," Available at https://www.telegraph.co.uk/technology/3358263/Computer-virus-infects-International-Space-Station-laptops.html (2020/10/15).

[89] P. K. Martin, "Inadequate security practices expose key NASA network to cyber attack," Available at https://oig.nasa.gov/audits/reports/FY11/IG-11-017.pdf (2020/10/15).

[90] P. Horrocks, "Stop the blocking now," Available at https://www.bbc.co.uk/blogs/theeditors/2009/06/stop_the_blocking_now.html (2020/10/15).

[91] K. Mizokami, "North korea is jamming gps signals," Available at https://www.popularmechanics.com/military/weapons/a20289/north-korea-jamming-gps-signals/ (2020/10/15).

[92] "NASA cybersecurity: An examination of the agency's information security," Available at https://oig.nasa.gov/docs/FINAL_written_statement_for_%20IT_%20hearing_February_26_edit_v2.pdf (2020/10/07), Tech. Rep., Feb 2012.

[93] J. Finkle, I. Klotz, J. Menn, and J. Wolf, "NASA says was hacked 13 times last year," Available at https://www.reuters.com/article/us-nasa-cyberattack-idUSTRE8211G320120303 (2020/10/07).

[94] B. Goertz, "Deutsche welle satellite transmissions jammed," Available at https://www.dw.com/en/deutsche-welle-satellite-transmissions-jammed/a-14843697 (2020/10/15).

[95] R. C. Samples, "The state of NASA's cybersecurity," Available at http://www.spacesafetymagazine.com/media-entertainment/state-nasas-cybersecurity/ (2020/10/15).

[96] T. Colakov, "JAXA computer virus adds to growing cyber security concerns in space," Available at http://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/jaxa-computer-virus-adds-growing-cyber-security-concerns-space/ (2020/10/15).

[97] E. Protalinski, "NASA, ESA confirm hacks; The Unknowns says systems patched," Available at https://www.zdnet.com/article/nasa-esa-confirm-hacks-the-unknowns-says-systems-patched/ (2020/10/15).

[98] M. Emanuelli, "Epsilon rocket data stolen by hackers," Available at http://www.spacesafetymagazine.com/aerospace-engineering/cyber-security/epsilon-rocket-data-stolen-hackers/ (2020/10/15).

[99] K. Ahrens, "Hacker greifen deutsches zentrum für luft- und raumfahrt an," Available at https://www.ingenieur.de/technik/wirtschaft/verbraucherschutz/hacker-greifen-deutsches-zentrum-fuer-luft-raumfahrt-an/ (2020/10/15).

[100] P. B. de Selding, "Eutelsat blames Ethiopia as jamming incidents triple," Available at https://spacenews.com/40818eutelsat-blames-ethiopia-as-jamming-incidents-triple/ (2020/10/15).

[101] "Successful cyber attack highlights longstanding deficiencies in NOAA's IT security program," Available at https://www.oig.doc.gov/OIGPublications/OIG-16-043-A.pdf (2020/10/08), Tech. Rep., Aug 2016.

[102] M. Gruss, "NOAA admits to cyberattack on satellite data networks," Available at https://spacenews.com/42561noaa-admits-to-cyberattack-on-satellite-data-networks/ (2020/10/08).

[103] K. Zetter, "Russian spy gang hijacks satellite links to steal data," Available at https://www.wired.com/2015/09/turla-russian-espionage-gang-hijacks-satellite-connections-to-steal-data/ (2020/10/12).

[104] M. Lennon, "Russian-speaking turla attackers hijacking satellite internet links," Available at https://www.securityweek.com/russian-speaking-turla-attackers-hijacking-satellite-internet-links (2020/10/12).

[105] S. Tanase, "Satellite turla: Apt command and control in the sky," Available at https://securelist.com/satellite-turla-apt-command-and-control-in-the-sky/72081/ (2020/10/12).

[106] G. Corera, "How france's TV5 was almost destroyed by 'russian hackers'," Available at https://www.bbc.com/news/technology-37590375 (2020/10/12).

[107] D. Winder, "Confirmed: NASA has been hacked," Available at https://www.forbes.com/sites/daveywinder/2019/06/20/confirmed-nasa-has-been-hacked/ (2020/10/07).

[108] "Cybersecurity management and oversight at the Jet Propulsion Laboratory," Available at https://oig.nasa.gov/docs/IG-19-022.pdf (2020/10/07), Office of Inspector General, Tech. Rep., Jun 2019.

[109] M. K. Mithun, "ISRO computer had malware, could've been hacked, say researchers," Available at https://www.newindianexpress.com/cities/hyderabad/2018/mar/12/isro-computer-had-malware-couldve-been-hacked-say-researchers-1785758.html (2020/10/10).

[110] N. Villeneuve and J. T. Bennett, "Xtremerat: Nuisance or threat?" Available at https://www.fireeye.com/blog/threat-research/2014/02/xtremerat-nuisance-or-threat.html (2020/10/12).

[111] "Oninformation security incident of march 10, 2018," Available at https://www.isro.gov.in/sites/default/files/on-is-incident-istrac.pdf (2020/10/10).

[112] T. Starks, "Chinese hackers targeting satellite and defense firms, researchers find," Available at https://www.politico.com/story/2018/06/19/

chinese-hackers-targeted-satellite-and-defense-firms-researchers-find-1442591 (2020/10/12).

[113] "China-based hacking campaign is said to have breached satellite, defense companies," Available at https://www.cnbc.com/2018/06/19/china-based-hacking-breached-satellite-defense-companies-symantec.html (2020/10/12).

[114] M. Harris, "Ghost ships, crop circles, and soft gold: A GPS mystery in shanghai," Available at https://www.technologyreview.com/2019/11/15/131940/ghost-ships-crop-circles-and-soft-gold-a-gps-mystery-in-shanghai/ (2020/10/12).

[115] "Tesla model s and model 3 prove vulnerable to GPS spoofing attacks as autopilot navigation steers car off road, research from regulus cyber shows," Available at https://www.bloomberg.com/news/articles/2019-06-19/threat-of-gps-spoofing-for-autonomous-cars-seen-as-overblown (2020/10/12).

[116] G. Spocchia, "Mysterious GPS signals reveal ghost ships sailing in wide circles off san francisco coast," Available at https://www.independent.co.uk/news/world/americas/gps-signals-phantom-ships-san-francisco-a9556966.html (2020/10/12).

[117] H. Osborne, "Phantom boats drawing 'GPS crop circles' keep appearing off the coast of san francisco," Available at https://www.newsweek.com/ships-gps-crop-circles-san-francisco-1509012 (2020/10/12).

[118] D. M. Harland and R. D. Lorenz, *Space Systems Failures Disasters and Rescues of Satellites, Rockets and Space Probes*. Springer, 2005.

[119] B. Schneier, "Cyberattacks against nasa," Available at https://www.schneier.com/blog/archives/2008/12/cyberattacks_ag.html (2020/10/07).

[120] P. Rosenzweig, "The alarming trend of cybersecurity breaches and failures in the u.s. government," Available at https://www.heritage.org/defense/report/the-alarming-trend-cybersecurity-breaches-and-failures-the-us-government (2020/10/07), May 2012.

[121] K. Epstein, "Network security breaches plague nasa," Available at http://www.kepstein.com/2008/11/20/network-security-breaches-plague-nasa/ (2020/10/07).

[122] D. Campbell, "Cyber sillies," Available at https://www.theguardian.com/uk/1999/may/20/military.defence (2020/10/07).

[123] "Did hackers hijack a british military satellite?" Available at http://news.bbc.co.uk/2/hi/science/nature/288965.stm (2020/10/07).

[124] D. Albright, P. Brannan, and C. Walrond, "Did Stuxnet take out 1,000 centrifuges at the Natanz Enrichment Plant?" Available at https://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf (2021/08/21), Tech. Rep., Dec 2010.

[125] G. Buesnel, J. Pottle, M. Holbrow, and P. Crampton, "Make it real." *GPS World*, vol. 27, no. 11, pp. 24 – 29, 2016.

[126] W. Myrick, "GPS beamforming with low cost RTL-SDRs," Available at https://www.gnuradio.org/grcon/grcon17/presentations/gps_beamforming_with_low_cost_rtl_sdrs/Wil-Myrick-GPS-Beamforming-with-Low-Cost-RTL-SDRs.pdf (2020/10/14).

[127] ——, "GPS beamforming with low cost RTL-SDRs," Available at https://github.com/B44D3R/SDR-GPS-SPOOF (2020/10/14).

[128] D. Hambling, "Ships fooled in GPS spoofing attack suggest russian cyberweapon," Available at https://www.newscientist.com/article/2143499-ships-fooled-in-gps-spoofing-attack-suggest-russian-cyberweapon (2020/10/14).

[129] A. Ramm and V. Zykov, "Ministry of defense will jam GPS from cell towers," Available at https://iz.ru/news/628766 (2020/10/13).

[130] B. Hendrickx, "Ekipazh: Russia's top-secret nuclear-powered satellite," Available at https://thespacereview.com/article/3809/1 (2020/10/14).

[131] B. Bailey, R. J. Speelman, P. Doshi, N. C. Cohen, and W. A. Wheeler, "Defending spacecraft in the cyber domain," Available at https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf (2021/03/26), Tech. Rep., Nov 2019.

[132] B. Bailey, "Establishing space cybersecurity policy, standards, and risk management practices," Available at https://aerospace.org/sites/default/files/2020-10/Bailey%20SPD5_20201010%20V2_formatted.pdf (2021/04/28), Tech. Rep., Oct 2020.

[133] J. Oakley, *Cybersecurity for Space: Protecting the Final Frontier*, 1st ed., 2020.

[134] S. Skorobogatov, "Breakthrough silicon scanning discovers backdoor in military chip," in *Cryptographic Hardware and Embedded Systems Workshop (CHES)*, 09 2012.

[135] N. Aeronautics and Administration, "NASA open source projects repository: core Flight System," Available at https://code.nasa.gov/?q=core%20flight (2021/09/28).

[136] ——, "core Flight System," Available at https://cfs.gsfc.nasa.gov/ (2021/09/28).

[137] Amazon Web Services, "FreeRTOS," Available at https://freertos.org/ (2021/09/28).

[138] "LibreCUBE," Available at https://librecube.org/ (2021/09/28).

[139] "Libre Space Foundation projects," Available at https://libre.space/projects/ (2021/09/28).

[140] "Two-line element set," Available at https://en.wikipedia.org/wiki/Two-line_element_set (2021/04/24).

[141] J. Pavur and I. Martinovic, "The Cyber-ASAT: On the impact of cyber weapons in outer space," in *2019 11th International Conference on Cyber Conflict (CyCon)*, vol. 900, 2019, pp. 1–18.

[142] "Orbit data messages," The Consultative Committee for Space Data Systems, Recommended Standard CCSDS 502.0-B-2, Nov 2009. [Online]. Available: https://ccsds.org

[143] "Conjunction data messages," The Consultative Committee for Space Data Systems, Recommended Standard CCSDS 508.0-B-1, Jun 2013. [Online]. Available: https://ccsds.org

[144] M. Azriel, "Roscosmos makes it official: Proton downed due to upside down sensors," Available at http://www.spacesafetymagazine.com/space-disasters/rocket-failure/roscosmos-official-proton-downed-due-upside-sensors/ (2021/09/28).

[145] S. Clark, "Arianespace traces cause of vega launch failure to 'human error'," Available at https://spaceflightnow.com/2020/11/17/arianespace-traces-cause-of-vega-launch-failure-to-human-error/ (2021/09/28).

[146] G. Maral, M. Bousquet, and Z. Sun, *Satellite communications systems : systems, techniques and technology*, sixth edition.. ed., 2020.

[147] J. Pavur, D. Moser, V. Lenders, and I. Martinovic, "Secrets in the sky: On privacy and infrastructure security in DVB-S satellite broadband," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, ser. WiSec '19. New York, NY, USA: Association for Computing Machinery, 2019, p. 277–284. [Online]. Available: https://doi.org/10.1145/3317549.3323418

[148] "CCSDS space link protocols over ETSI DVB-S2 standard," The Consultative Committee for Space Data Systems, Recommended Standard CCSDS 131.3-B-1, Mar 2013. [Online]. Available: https://ccsds.org

[149] "Security architecture for space data systems," The Consultative Committee for Space Data Systems, Recommended Practice CCSDS 351.0-M-1, Nov 2012. [Online]. Available: https://ccsds.org

[150] "Unified space data link protocol," The Consultative Committee for Space Data Systems, Recommended Standard CCSDS 732.1-B-1, Oct 2018. [Online]. Available: https://ccsds.org

[151] "Space packet protocol," The Consultative Committee for Space Data Systems, Recommended Standard CCSDS 133.0-B-2, Jun 2020. [Online]. Available: https://ccsds.org

[152] "Space data link security protocol," The Consultative Committee for Space Data Systems, Recommended Standard CCSDS 355.0-B-1, Sept 2015. [Online]. Available: https://ccsds.org

[153] A. Satapathy and J. Livingston, "A comprehensive survey on SSL/TLS and their vulnerabilities," *International Journal of Computer Applications*, vol. 153, pp. 31–38, 11 2016.

[154] G. Caparra, S. Ceccato, F. Formaggio, N. Laurenti, and S. Tomasin, "Low power selective denial of service attacks against gnss," 09 2018.

[155] C. Gibson, "Iot and satellite security in the age of 5g," Available at https://www.trendmicro.com/en_us/research/18/f/attack-vectors-in-orbit-need-for-satellite-security-in-5g-iot.html (2020/10/12).

[156] Y. Afek, M. Merritt, and G. Taubenfeld, "Benign failure models for shared memory," in *International Workshop on Distributed Algorithms*. Springer, 1993, pp. 69–83.

[157] R. H. Zielinski, I. Worley, Robert M, D. S. Black, S. A. Henderson, and D. C. Johnson, "Star tek - exploiting the final frontier: Counterspace operations in 2025," Tech. Rep., 1996. [Online]. Available: http://www.dtic.mil/docs/citations/ADA392588