Space Policy 59 (2022) 101458

Contents lists available at ScienceDirect

Space Policy

journal homepage: www.elsevier.com/locate/spacepol

A World without Satellite Data as a Result of a Global Cyber-Attack

Charlotte Van Camp, Walter Peeters*

International Space University (ISU), Parc d'innovation, 1 rue Jean-Dominique Cassini, 67400, Illkirch-Graffenstaden, France

ARTICLE INFO

Article history:
Received 23 February 2021
Received in revised form
16 August 2021
Accepted 11 October 2021
Available online 31 December 2021

Keywords:
Satellite breakdowns
Kessler syndrome
Carrington effect
Cyberthreats
Survey
Economic consequences
TCBM
Cybersecurity

ABSTRACT

The probability that all satellites in space fail simultaneously is by experts qualified as highly improbable but not excluded. In literature, we find two major potential risks that can cause this, a mega solar storm (so-called Carrington Effect) or a space debris chain reaction (called the Kessler effect). However, a survey with experts described in detail in this article points out an equally harmful and even more presently plausible scenario, namely cyber-attacks.

Irrespective of the probability, it deserves an attempt to imagine the economic major damage that such total satellite collapse would represent for society. It will clearly illustrate our dependency on satellite data and areas that may be less obvious at first sight. Therefore, the consequences of such a scenario, even if there is a low probability, are explored under this assumption.

Cyber-attacks on satellites have already taken place on several occasions, from which a few past and recent ones are reported in this article. In particular, satellite operators and military organizations are not frequently reporting such attacks publicly given the loss of confidence by the clients or the general public respectively. There seems to be no solution to the existing problem of pinpointing the source of an invisible and non-observable yet successful attack. We can say without hesitation that, with the investments in cyberwarfare and improved techniques, such threats will become more frequent, and unfortunately, more effective soon.

This article will discuss potential technical countermeasures such as Rapid Response programs, as well as policy-oriented measures. In the latter, the effectiveness of agreements in this field is questionable. Therefore, emphasis will be put on Transparency and Confidence Building Measures (TCBM).

1. Introduction

"You wake up and turn on the TV. Your usual shows aren't airing. You flip on the radio and learn that Paris and Tokyo stock markets have closed. Back on TV CNN is trying to use Skype in an attempt to cover what's happening in the world following a solar super storm.

In a US bunker, the military has lost contact with armed drones flying over hostile areas. Loss of global communication satellites makes it difficult to send commands and surveillance data to soldiers, ships and aircraft, rendering them vulnerable to attack.

Throughout the day more challenges arise. First responders don't have access to their location systems. Delays in ground and air traffic begin to develop. Systems that depend on GPS[1] time stamps — ATM[2]s, power grids, computer-data and cell-phone networks begin to fail, and the cloud becomes unstable. The internet soon collapses." [1].

This is a good journalistic summary of a presentation given by the Norwegian solar physicist Pål Brekke [2]. It demonstrates well the two main angles we can also find in numerous articles on this topic, namely.

- The evident relation with solar storms
- The potential impact on military capabilities

As far as military aspects are concerned, a lot of studies are related to the dependence of modern weapons systems on accurate navigation systems. Protection against outside effects is, in

* Corresponding author.
E-mail address: walter.peeters@isunet.edu (W. Peeters).

[1] GPS = Global Positioning System (US-provided navigation system).
[2] ATM = Automated Teller Machine (also referred to as cash-dispensers).

https://doi.org/10.1016/j.spacepol.2021.101458
0265-9646/

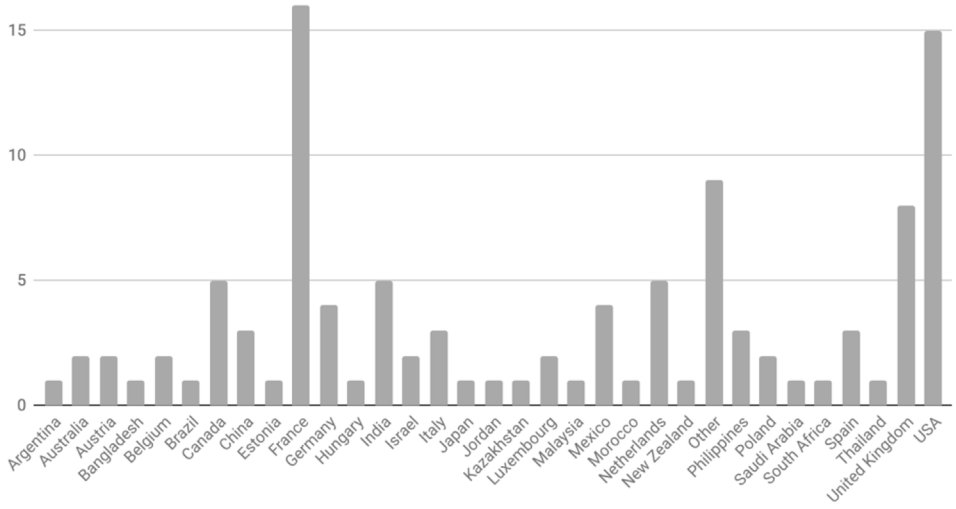

Fig. 1. Geographical distribution of survey respondents [9].

particular for the case of GPS, studied in large detail. In his book on GNSS[3] interferences and threats, Dovis [3] emphasizes the risks for jamming devices such as spoofing (i.e., the transmission of counterfeit GNSS signals) and GNSS receiver deception and describes extensively countermeasures that can be taken.

However, not only malicious manipulations can cause a lot of damage. A simple accidental uploading at an incorrect time during a standard operational procedure in January 2016 caused many errors and malfunctioning of radio equipment, digital radio, and even in power grids during some 12 h [4].

Suppose we add to this the enormous need for bandwidth capacity for military purposes, which is exponentially increasing due to the use of drones and unmanned vehicles. In that case, it is not surprising that military tactics are increasingly targeting procedures for a warfare scenario based upon limited space data support [5]. In this article, military commanders are quoted to state that "We developed an overdependence on high-bandwidth communication systems and the contractors required to run them." As an answer to this, large-scale training exercises with degraded communications and GPS capabilities have now been regularly introduced.

Whereas on the one hand, increased international cooperation and agreements shall be pursued, policy experts such as Scott Pace strongly suggest, in parallel, not to ignore increased protective measures as well:

> *Improving resilience can consist of both "material" and "non-material" solutions. The former includes measures such as hardening space and ground systems against physical and cyber-attacks. The latter can include development of alternative means of mission performance, such as the use of allied or commercial systems with assets in space or on the ground. This will strengthen deterrence and improve stability more than purely symbolic gestures, such as signing ceremonies or declarations* [6].

In analogy, also our economy is becoming increasingly dependent on reliable space data. Whereas this is less obvious such as in the case of banking transactions, it is evident that with an increasing dependency of GNSS for automated transport means and collision avoidance systems, we need to pay attention to the economic aspects.

As mentioned before, a total blackout of all satellites is considered very unlikely. Traditionally two potential scenarios were considered, namely a very powerful solar storm and a space debris chain reaction possibility (which became better known to the general public via the movie 'Gravity'). Both Dvorsky [7] and Johnson [8] contest this theory and consider cyber-attacks as an even bigger threat.

2. Methodology of the research

In order to learn more about the perceived threats, a survey was made addressing space experts in this field or were confronted with these threats, both governmental as well as satellite operators. For the purpose of getting a broad opinion on the risks of threats to the space sector in the future, a questionnaire was developed and distributed to Space experts and policymakers, in particular, linked internationally to the ISU (International Space University) alumni environment.

For reasons of methodology, a wide range of topics was forwarded for consideration in the questionnaire, even if the survey developers assumed that the risks were not at the same level.

The study is reported in Ref. [9] and is based upon the analysis of 109 responses, with 63.9% respondents from the private sector, and 36.1% of the public sector. This includes space professionals working in space companies and government organizations in Africa, Asia, Europe, Latin America, the Middle East, North America, and Oceania.

Answers per country of the respondents were distributed as per Fig. 1.

The aim of the questionnaire was to measure whether space professionals see these subjects as a threat to space activities or whether they gauge these subjects to be at low risk. Fig. 2 below demonstrates the results to the question "how would you rate following threats on a scale from 1 to 7?".

Cyber threats are seen as the main threat among these space professionals. On a scale of one to seven (with one indicating low risk and seven indicating a high risk), 30.3% of the respondents marked cyber threats with seven, and 93.6% have responded with a rate of four or higher.

Space debris and lack of space traffic management also received high-risk rates, with 87.1% of the respondents rating space debris

[3] GNSS = Global Navigation Satellite Systems (global term for satellite constellations providing positioning and navigational (PNT) services.

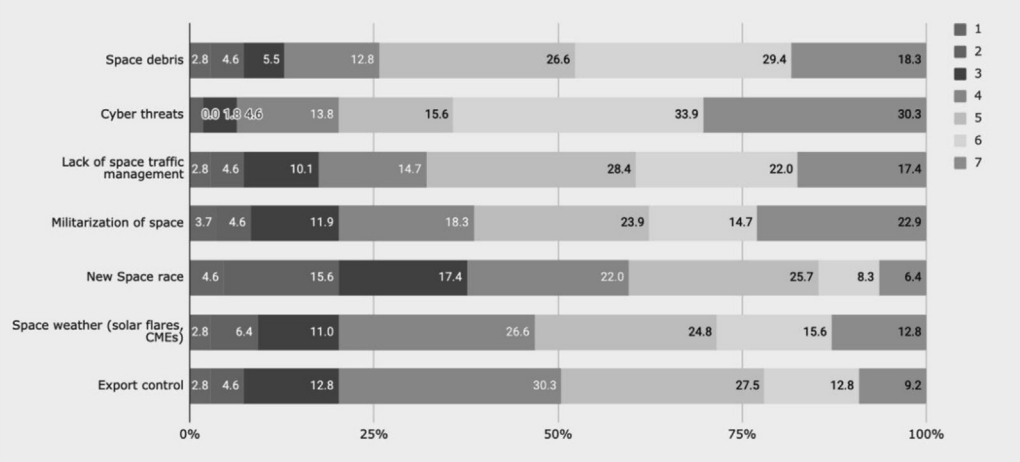

Fig. 2. Rating of threats according to respondents on a 7-point scale [9].

with four or higher, and 82.5% rating four or higher, for lack of space traffic management.

Some of the threats, such as export control, space weather, and militarization of space, received a relatively high number of responses for level 4 compared to other threats in the questionnaire. This can indicate that professionals are more neutral about the risks related to export control (30.3%), space weather (26.6%), and militarization of space (18.3%) compared to other subjects.

Only 40.4% of the respondents gave a rate between five and seven for the possible threat of 'a new space race'. Compared with the other threats of the questionnaire, this is the topic in which space professionals see the least risk. Except for export control (49.5%), most of the respondents gave a rate higher than four for all other threats. Thus, space weather (53.2%), the militarization of space (61.5%), lack of space traffic management (67.8%), cyber threats (79.8%), and space debris (74.3%) were given a rating between five and seven.

Comparing the results to the questionnaire between the public sector and private sector space professionals, one can conclude that there are no major differences in the responses to the threats. However, more respondents from the private sector suggested cyber threats to be the highest risk (34.78%) compared to the public sector (22.5%).

Let us add to this questionnaire a technical dimension: the chances of these threats completely blocking all satellite data? Therefore, as the next step in our systems approach, we evaluate the different threats about a potential global shut-down of all satellite services, as per Table 1.

If we combine the results, we can draw a few interim conclusions, namely:

- The Kessler Syndrome is theoretically a threat, although experts do not estimate the probability as very likely.
- Recent mega storms did not affect satellite systems, and the intensity of the Carrington event is still debated.
- The Kessler syndrome and the Carrington event are well described and documented in literature, but the probabilities are considered very low.
- On the other hand, cyber-attacks on satellites have an increased probability of having a strong impact, also as the knowledge behind this is rapidly increasing, in particular in military organizations. In addition to this, this threat is controlled and can be executed from Earth-based systems.

In the next chapter, we will briefly describe the perceived main risks, namely the Kessler Syndrome, the Carrington effect, and in more detail, a global cyber-attack threat.

3. Description of potential threats

3.1. Space debris: the Kessler Syndrome

As the number of satellites in Earth's orbit increases, the density of these objects will also increase, which might cause a chain reaction of further collisions. More specifically, the fragmentation debris caused by a collision will lead to a domino effect of new collisions and result in a debris belt around the Earth. This event is

Table 1
Evaluation of the probability for a global blackout per threat.

Threat	Global satellite shutdown	Partial satellite shutdown	Manageable effect	Rationale
Kessler Syndrome		XX		GEO satellites may not all be affected
Carrington Effect		XX		Satellites protected thanks to more resilient electronic components and countermeasures in view of early warning via solar observation networks
Cyber-attacks	XX			Effect is increasingly threatening, retaliation and escalation possible in case one nation is originating such attacks.
Space traffic management			X	Mainly local effects although with potential collateral damage
New Space Race			X	Unlikely to affect commercial satellites
Space Militarization		X		Considerable impact on military satellites, but limited on commercial satellites
Export Control			X	Reduced chance for a global impact

also called the Kessler Syndrome, as predicted by Kessler and Cour-Palais in 1978 [10].

As mitigation of this threat, systems such as TCBM (Transparency and Confidence Building Measures) are also, in this case, proposed as international countermeasures based upon international agreements [11].

3.2. Solar storms: the Carrington Effect

Space weather or variable conditions in space and on the sun can impact the technology we use on Earth [12]. Solar flares, explosions that occur when magnetic energy surges around sunspots and releases hot plasma, are usually followed by Coronal Mass Ejections (CMEs). Coronal Mass Ejections are high-volume releases of hot plasma that move through the sun''s corona at extreme velocities.

Both solar flares and CMEs can lead to geomagnetic storms, which can cause satellite damage, satellite loss, and communications problems. An example of such a geomagnetic storm is the Carrington event, which took place in 1859 [13]. It was the worst geomagnetic storm recorded in 500 years and caused machines to burst into flames, telegraph malfunction, and power shortage.

Also, for this case, suggestions are being made to improve action plans in existing international solar observation agreements to provide an early possibility for satellite operators to take possible protective countermeasures [14].

3.3. Special emphasis: cyber-attacks on space systems

Cybersecurity relies on information technologies developed from all over the world, and both advanced and emerging nations are vulnerable to attacks. There are different classification groups of cyber threats against space-based systems. The purpose behind the attack could vary from obtaining intellectual property from another state to terrorist groups and individual hackers seeking financial gain. It may also cause a reduction in national security, corrupt communication, navigation, and observation satellites, or destruct a complete space vehicle.

There are other examples of cyber-attacks on infrastructures that rely on space-based systems. For instance, in a Chatham report that discusses the threats and consequences of cyber-attacks on nuclear weapon systems, the authors explain that the digitization of systems and new technologies come with many benefits. However, the vulnerabilities and the exacerbated risks that come with them must also be addressed [15]. The risk of an attempted cyber-attack on a nuclear system, is considered to be relatively high. North Korea's missile systems have been reported to be infiltrated by the United States on multiple occasions, further causing test failures. Mostly command, control, and communications systems are vulnerable to cyber-attacks [15].

Many countries are looking into counter-space capabilities that include electronic and cyber methods. Compared to anti-satellite (ASAT) capabilities, an interference with a satellite through a cyber-attack can be carried out in a cheaper, faster, and more difficult to notice manner [16].

Cyber-attacks, together with drones and automated warrior-robots, are increasingly considered a global threat to stability in the world. Some authors [17] point out that taking humans out of the loop has a certain appeal to politicians. For example, a drone that has been destroyed does not have a pilot on board that can be captured and used as a political bargaining chip or a PR element. Same for cyber-attacks that are not at all easy to attribute to a specific attacking state and can be launched from any spot in the world.

If we refer to satellite cyber-attacks, we often relate this to accessing the satellite or satellite system via the ground stations. Several attempts, often considered by cyber-experts as experimental tests and preparatory, are known but not widely reported by satellite operators for obvious commercial reasons.

There are, however, also direct invasive means of cyber-attacks, often with rather simple means. A NATO report [18] classifies those as follows:

- *Jamming is the intentional interference with signal transmission and reception using electromagnetic signals. In particular, GNSS (Global Navigation Satellite Systems, like GPS) are vulnerable to this type of attacks.*
- *Spoofing is used to manipulate the information about the location and position of a satellite. A particularity of this attack is that it is relatively difficult to detect fast and can cause immense damage on critical infrastructure such as national power grids and financial operations before being (in most cases therefore indirectly) detected.*
- *Dazzling is a way of blinding a satellite with a laser. In extreme cases the laser can even be used as a more invasive attack and burn satellite sensors and other subsystems.*

A number of cyber-attacks were reported in previous articles, Like the one on the US-German ROSAT satellite in 1998 [19], the hacking of the Skynet network in 1999 [20]; the one on US satellites via a Norwegian ground station in the period 2007–2008 [21], as well as hacking a NOAA satellites in 2014 [22]. As those events were not fully documented, in chapter four, we will concentrate on more recent, fully documented ones.

In contrast to military satellites that are commonly designed so that the security aspect is included, commercial satellites are generally more vulnerable to attacks because of a lack of awareness and implementation of security.

Often, manufacturers of satellites use off-the-shelf technology to make the costs more reasonable. Some of these components can be screened by hackers for vulnerabilities in open-source technology and software. Hacking some of the CubeSats could also be easily done by using specialized ground antennas. Satellites are controlled from ground stations that run computers with softwares that are vulnerable to potential hackers.

Cyber specialists also point out the relation with New Space projects, where creative applications in lower Earth orbits replace Geostationary satellites. As it was reported, the conference concluded the following:

> *"New and start up satellite companies should have a higher sense of what the cyber risks are going into the market and understand that they are not just building satellites, they are building an information ecosystem, that if breached and used for the wrong intent could have catastrophic consequences and place millions of lives in danger"* [23].

The danger for cyber-attacks is increasingly becoming important, as the hacking 'technology' is under constant evolution, with cybersecurity only able to react posterior once the threats are evident.

Whereas in the past, mainly the nations with important financial, military expenses were considered as a large threat, one should not ignore that hackers can be found all over the world and can operate well protected from different, also emerging countries. A recent example is the EU countries creating infrastructure on cybersecurity [24].

4. Recent cyber-attack threats with broader impact and developments

The impact of a cyber-attack on a global scale can be illustrated with attacks that caused enormous damage nationwide in Estonia and Ukraine. Estonia is the first country globally that became a victim of multiple nationwide cyber-attacks in 2007 [25]. The cyber-attacks started after ethnic Russians went into a protest against the Estonian government for removing a statue built by the former Soviet Union [26]. The attacks lasted for weeks and took down all electronic infrastructure, digital services, and government bodies. As a consequence, ATMs stopped functioning, digital communication and news broadcasting were made instantly impossible. The country has improved its cybersecurity ever since and now ranks among the top nations in the International Telecom Union (ITU) Global Cybersecurity Index [27].

Like Estonia, Ukraine became a victim of a nationwide- and one of the most devastating global cyber-attacks. Until today it is still not confirmed who was responsible for the so-called 'NotPetyas' attack [28]. However, Ukraine was hit hardest with 80% of the infection [29]. The attack blocked the Ukrainian government agencies, banks, and airports from digital services and operations [30]. The worm then spread beyond Ukraine, unintentionally causing damage to hundreds of companies in over 60 countries [29].

Although no people got physically injured due to the 'NotPetya's' attack, the financial losses estimations are at 10 billion USD [28]. Table 2 below provides an overview of six companies that became a victim of NotPetya.

Large-scale attacks have continued to occur in Ukraine. Another nationwide cyber-attack affected power distribution to 230 000 Ukrainians. Meanwhile, Estonians have been supporting the Ukrainian government to improve their cybersecurity capabilities [30].

The Colonial Pipeline company, one of the largest fuel carrier companies in the United States, became a victim of a cyberattack in May 2021. The company, which transports refined oil products from the gulf coast to the East coast, had to shut down their 8850 km pipeline. The attack was carried out by a Russian hackers group named 'Darkside', who threatened to leak the 100 gigabytes of data they stole from the Colonial Pipeline [31]. Initially, it was announced that the Colonial Pipeline would not be paying the ransomware to Darkside. However, the company eventually paid a ransom of 75 bitcoins, worth approximately 5 million USD, so they could resume operations [32]. The Federal Bureau of Investigation (FBI), involved in the case, later announced that they strongly discourage companies from paying ransoms because it does not guarantee that data will be restored. On the contrary, it might encourage hackers to carry out attacks where they ask for higher amounts of money or cryptocurrencies [33].

More recently, on July 5th, 2021, the largest ransomware attack took place, affecting approximately 200 firms and one million systems globally. Some of the confirmed victims include the Swedish supermarket Coop, disturbing 500 of its stores, several schools in New Zealand, and two Dutch IT firms. The attackers named 'Revil' demanded 70 million USD in bitcoin [34]. In the case of ransomware in cryptocurrencies through blockchain, it becomes even more complex to track the payment.

Estimates of global financial losses due to cyber-attacks in 2021 are at 6 trillion USD [35]. It is only a matter of time before the next global cyber-attack occurs. If inflicted because of political, ethnic, or personal conflict, the question remains what safety measures there are against a sophisticated group of hackers that aim to shut down much larger assets.

Table 2
Companies that are victims of NotPetya Cyber-attack.

Company	Reported Damage
Merck	$870,000,000
FedEx	$400,000,000
Saint Gobain	$384,000,000
Maersk	$300,000,000
Mondelēz	$188,000,000
Reckitt Benckiser	$129,000,000

5. Multilateral initiatives with regards to cyber-attacks

International law, the principle of nonintervention and the principle of sovereignty are all applicable in states' cyber activities [36]. However, there is a lack of agreement internationally around *how* they are applicable. Several multilateral initiatives at diplomatic levels have been carried out to mitigate the risks of cyber-attacks [36].

- The Tallinn Manual is one of the most comprehensive documents around this topic and includes the concepts of sovereignty and nonintervention.
- The United Nations Group of Government Experts (UN GGE) have also been discussing this topic since 2004, further establishing an Open-Ended Working Group in 2018 that invites all UN member states to the discussion [36].
- In the PAROS (Prevention of an Arms Race in Outer Space) 2019, cyber-attacks are also referred to as a tool to disable space objects, which, in view of the International Committee of the Red Cross, is considered as an attack under International Humanitarian Law (IHL) [37].

Cybersecurity matters recently have been raised between US President Joe Biden and the Russian President Vladimir Putin. President Joe Biden expressed that they expect other countries to take action when ransomware attacks from their ground are carried out on US companies, especially if the US authorities can provide sufficient information prior to the attack about those cyber groups. The Russian government stated that they support cooperation between the two countries in the cybersecurity domain "with respect to international law" [38].

There are few cases where people were charged for cyber-attacks. In October 2020, six computer hackers of the Russian military intelligence were charged in the United States for deploying destructive malware such as NotPetya, causing global financial and economic losses. The computer hackers were also charged with conspiracy, identity theft, wire fraud, disruptive cyber-attacks on the 2016 French elections, cyber-attacks on Georgian government entities and Ukrainian critical infrastructures, just to name a few [39].

Chinese scholars, obviously in line with official consent, have pleaded for more transparency and confidence-building measures (TCBMs) [40].

TCBMs encourage nations to be transparent about their space-related activities and their intentions. Several space technologies are dual-use, making it harder to understand their purposes. For instance, a misunderstanding after a satellite loss can cause political conflict on Earth or cyberspace [41]. This is why TCBMs play an important role in the safety of outer space activities. They remain non legally binding but have proven to be important contributors to the prevention of weaponization or an arms race in outer space. However, it would be suggested to go beyond TCBMs and define clearer international laws regarding cyber-attacks on space systems, also in the framework of non-state actors.

At times when cyber-attacks were addressed in the space cyber domain, there has been a lack of consistency in the range of vulnerabilities and reported events. This led to a false understanding of potential risks and countermeasures that need to be taken into account to tackle these issues [42].

In 2019, The UK drafted an initiative UN resolution that is aimed at reducing space threats through responsible behavior in space [43]. In the UNGA 75th session, UNGA noted the fast-growing technological changes in space systems and their effects on international security. It was also stressed that if the use of these technologies on the ground or in space are inconsistent with the ambition of sustaining an internationally safe and secure environment, that these actions may be perceived as threats and further undermine international peace and security on Earth. UNGA highlighted the necessity for all nations to cooperate and develop new rules that contribute to establishing a more transparent and stable space environment [44].

6. The economic impact of a global space data blackout

Even if the probability of a complete shutdown of space data is very low, countermeasures have been studied, which clearly show that the possibility is taken seriously, in particular by military organizations. In broad terms, we have to consider two main effects.

- Rapid replacement of damaged satellites
- Economic collateral effects

6.1. Satellite replacement

In 2007, the US DOD created the ORS (Operationally Responsive Space) Organization [45]. This was triggered by a Policy Directive of 2005 stating the need to:

> "demonstrate an initial capability for operationally responsive access to and use of space — providing capacity to respond to unexpected loss or degradation to selected capabilities and/or to provide timely availability of tailored or new capabilities — to support national security requirements." [46].

ORS developed a modular approach with a stock of essential flexible subsystems and components to rapidly assemble and launch tailored satellites with dedicated launchers in a span of a few days. Although the prime objective was to create extra capacity in case of a conflict, the element of degradation of the existing military space capability was not disregarded.

Several operational launches took place from 2008 onward. The recent one reported, ORS-5, took place in 2017 [47], with other missions planned. Nevertheless, the extensive cost to keep a considerable stock of building blocks (with limited technological lifetime) remains a hurdle for this initiative.

In the event of a global loss of satellites, there is no doubt that authorities will prioritize replacing military satellite capacity in space.

The first replacements will probably take place with limited lifetimes-satellites operating in low orbit constellations. Eventually, modern weapon systems are too dependent on precision locations, and very soon, GNSS capacity will be needed next to surveillance and telecommunication capacity.

It is hard to estimate the cost of this replacement as there is a wealth of knowledge now that can accelerate the design process and cheaper components. Suppose we refer to a figure of approximately 25 Billion USD that the present GPS system has cost. We could compare it with a worldwide military spending annually in the order of 40 Billion USD. In that case, we can imagine that those military assets in space will be replaced in the range of several hundred billion dollars.

There will also be an immediate need in the civil protection sector to replace satellites for weather predictions, disaster management, aerial and sea safety surveillance-, and in general earth observation activities. Here, some reflections have been made about modular approaches with stocks of components to be able to react quickly.

The ability to respond to an arising need quickly cannot be satisfied by launchers and satellites already built and available. The only viable solution would be to have a stack of components readily available and produce smallsats for short missions. Having such a satellite available in a week's time is proposed by authors using modular launchers and satellite busses with 'plug-and-play' components [48]. The costs of such operation are evidently another obstacle, and components and integration may have to take place close to a launch site to meet the deadlines. At this moment, it is hard to imagine the organization that will be able to coordinate such effort (also geopolitically) and will have the power to impose priorities.

Also, the limited availability of micro-launchers at present and the rather obvious priority that will be given to launching strategically important government projects will, in such a case, force the industry to carry heavy investments over many years to create a semi-stable infrastructure. With a present commercial satellite manufacturing and launch sector activity in the order of 25 Billion USD worldwide [49], we can also here imagine an effort in the order of several hundred billion USD for early replacement and a robust infrastructure over a time span of 7−10 years.

6.2. Collateral damage

Whereas previously we discussed the direct replacement costs, there is no doubt that collateral damage will be even more important. Indeed, many operations and systems will not be able to operate without space data (and we need to point out that in the future, with drones and autonomous driving cars, this will become exponentially more complex).

If we take as an example the use of GPS, this was estimated equivalent to 0.3% of the US GDP in 2015 (and is surely higher now) [50]. If we focus on GNSS, we can list several economic factors for such activities such as:

- Precision agriculture
- Commercial fishing
- Open-pit mining to guide equipment
- Offshore energy exploration and development
- In first responder services
- In structural monitoring of dams and bridges

An absence of navigation tools will have a strong economic impact on these areas. Besides, there will be more invasive situations in other sectors, like:

- In aviation, for navigation and monitoring positions of aircraft and satellite-based augmentation systems
- Railroad train pacing systems for cruise control, positive train control to keep track of train location and movement authorities
- In marine transportation, for navigation, collision avoidance, communications, and situational awareness
- In vehicles with handheld and embedded devices for navigation and fleet management.

But probably, the most invasive economic effect will result from the sudden unavailability of timestamps. Indeed, precise timing and time synchronization, and frequency coordination (syntonization) is used most notably in broadcasting and communications, including both cell phones and traditional telephone applications and the internet, so packets arrive at the same time for power generation and distribution to locate problems, and in financial services for timestamping transactions.

In fact, the whole financial system will collapse within hours as it is based upon these timestamps, followed a few hours later by a breakdown of power grids, which are also driven by this precise synchronization. Also, many systems are indirectly depending on band-with or earth observation applications causing additional collateral damage. Still, the lack of navigation signals and timestamps will lead rapidly to dramatic situations in the course of hours.

Based upon a study [51], which assumed zero space data without any warning (irrespective of the probability if this can indeed happen), we could imagine the following timeline as per Tables 3 and 4, whereby T0 is the moment that all satellites would stop to work:

Table 3 shows the immediate effects. Traffic on the road relies on navigation guidance. Rarely, for longer distances, maps are consulted in advance. If suddenly there is no navigation system, cars and trucks will be completely lost, and we will immediately witness mega traffic jams. These unprecedented traffic jams will also block emergency services.

Other transport sectors like trains, ships, and planes will also lose the space data support. Major airlines will immediately ground their fleets. In general, the absence of GNSS navigation data will cause the first major visual effect.

A less obvious consequence will be linked to timestamp-based operations, which will be immediately aborted. Cash dispensers will not work anymore, and banks will be congested. Soon after, financial operations will stop, and stock markets will be affected, up to the point that they will have to be closed.

The same timestamp effect will heavily influence power system synchronization with increasing numbers of blackouts. This, in its turn, will increasingly influence transport chains of foods and medicaments.

Communication channels will be affected, and the lack of news will lead to panic reactions in terms of panic-food purchasing and even plundering. Remote areas will not be reachable, and, e.g., emergency plans will be made to evacuate ISS due to the increased risk.

Note that we are concentrating on the economic collateral effect, it is evident that military drones and jets will be grounded, and the overall military concept will require emergency measures.

In Table 4, we discuss follow-on effects. After one week, many companies will have to stop activities due to their dependency on space data or shortages in the supply chain. A gradual economic collapse will occur, leading to bankruptcies and unemployment, most probably leading to riots.

Depending on satellites' availability in stock (e.g., second flight models), governments will use existing launchers (mainly military) to try to restore some essential functions. However, to have functionally complete systems operational will require several months, and priority will be given to launch strategically important satellites. It will take a while before launchers are made available to launch commercial satellite constellations and the present absence of available micro-launchers.

We can assume that the first commercial smallsats in Low Earth Orbit will be operational before geostationary operations can be restored. By this time, the world economy will have suffered an unprecedented economic collapse, which will require years to be restored.

Table 3
Immediate consequence of a global shutdown (adapted from Ref. [51]).

T0	- All flights grounded, trains stopped, massive traffic jams (suddenly no GNSS signals) - Delayed intervention police/ambulances/fire brigades (no GNSS) - Cash-dispensers stop working (GNSS controlled)
T+ 2hrs	- Stock markets drop considerably - Congestion terrestrial communications and remote access (oceanic/polar) interrupted
T+ 7hrs	- News agencies and energy companies hit
T+ 11hrs	- No thunderstorm/hurricane/natural disaster warnings anymore
T+ 1 day	- Government limits public access to give priority to crisis communication - No public access to social media
T+ 2 days	- Financial transactions stop (no timestamp) - Breakdowns of power stations (uncontrolled overload)
T+ 3 days	- Power blackouts (no power synchronization) - Food and temperature-sensitive medicaments affected
T+ 4 days	- Food supply chain starts to break down - Panic buying of food, plundering
T+ 5 days	- Freshwater shortage - Tourism heavily affected

Table 4
Mid-term effects and remedial actions (adapted from Ref. [51]).

T+ 1 week	- Slow economic collapse - No funding transactions/no new contracts - ISS crew to be evacuated and ISS prepared for hibernation
T+ 2 weeks	- No forecasting of solar activity - Disrupted power grids (in particular if solar storm)
T+ 1 month	- Government will launch emergency satellites using existing military launchers
T+ 2 months	- Economy strongly affected - Communication companies bankrupt - Factories with complex delivery systems bankrupt
T+ 3 months	- Strategically important satellite constellations launched (military)
T+ 4 months	- Strong public push to increase space budgets immediately!
T+ 6 months	- New LEO constellations operational, also for civil use
T+ 12 months	- New GEO satellites operational

7. Conclusion

Experts consider a total collapse of all satellite systems at the same time unlikely but not impossible. Traditionally, two major effects were deemed potential causes for such a catastrophic scenario: a mega solar storm (Carrington effect) or a space debris chain reaction (Kessler Syndrome). A recent survey [32] teaches us that experts nowadays are more concerned about another threat, namely massive cyber-attacks on satellites.

It is improbable that any of these threats will irrevocably damage all satellites beyond repair. However, it is still useful to consider such a hypothetical case to analyze the effects and possibly reflect on strategies and countermeasures.

The most significant effect is linked to GNSS systems because navigation data are an integral part and a commodity of our infrastructure. An accurate timestamp is the basis for several financial operations and synchronizations, such as in power supply. Therefore, an absence of these data will lead to very dramatic supply chain situations and collapse our economic system.

The reliance of modern weapon systems on accurate GNSS data is well known, as well as the high bandwidth requirements for, e.g., drones. Both will therefore be severely influenced. Consequently, we can assume that governments will first try to restore a

minimum strategic infrastructure and use available resources for this, also in terms of launchers. This will additionally delay the restoration of commercial satellite data and increase the economic impact.

Several organizations have reflected on rapid, responsive systems as a potential countermeasure, like ORS in the United States of America. The cost of such systems is, however, a major obstacle for its development and extension. On the other hand, further developments of automated cars, planes, and ships will only increase the potential impact of such a global event and increase the resulting collateral damages and recovery costs in the future. This may motivate our society to reflect on such potential remedial countermeasure strategies.

In particular, young companies and start-ups should be made more aware of how to protect their satellites against cyber threats. Evidently, basic investments against cyberattacks are high and cannot be only carried by these young companies. More substantial work is necessary and needs to be done at levels such as ITU or Agencies like dedicated cyber-related guidelines, similar to general software design standards.

Taking into account the potential strong economic impact on the world economy as described, it looks evident that basic investments against cyber threats on space data are justified investments.

Increased international cooperation and information exchange can decrease the risks for a space debris effect and help protect satellites in time, thanks to earlier information on solar storms. In analogy, international agreements based upon transparency and confidence-building could protect to destroy a worldwide commodity, space data.

This TCBM strategy can only work when all parties, irrespective of their political convictions, adhere to it. Although very noble and worth pursuing, in the space tradition of redundancy, it is therefore recommended to, in parallel, invest in increased hardware protection against space debris and solar winds, as well as in increased software protection against cyber-attacks.

Funding

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] T. Cozzens, A day without satellites would affect all of us. [online] Available at: https://www.gpsworld.com/a-day-without-satellites-would-affect-us-all/ .(Accessed 22 June 2020).
[2] P. Brekke, A Day without Satellites, in: Proceedings of the 32nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2019), Miami, Florida, September 2019, pp. 1–69. [online] Available at: https://doi.org/10.33012/2019.16884. (Accessed 20 January 2021).
[3] F. Dovis (Ed.), GNSS Interference Threats and Countermeasures, Artech, Boston, 2015.
[4] Glass, D., What happens if GPS fails? [online] Available at: https://www.theatlantic.com/technology/archive/2016/06/what-happens-if-gps-fails/486824/. (Accessed 8 February 2021).
[5] Magnuson, S., U.S. Forces prepare for a 'day without space' [online] Available at: https://www.nationaldefensemagazine.org/articles/2014/2/1/2014february-us-forces-prepare-for-a-day-without-space. (Accessed 20 January 2021).
[6] S. Pace, Security in space, Space Pol. 33 (2) (August 2015) 55.
[7] G. Dvorsky, Hackers have Already Started to Weaponize Artificial Intelligence, Gizmodo, 9.11.2017 [online] Available at: https://gizmodo.com/hackers-have-already-started-to-weaponize-artificial-in-1797688425. (Accessed 10 February 2021).
[8] L. Johnson, Sky Alert! When Satellites Fail, , Springer, New York, 2013.
[9] C. Van Camp, How Do Space Professionals Feel in a Disharmonized Global Legal Environment? MSS IP, ISU, Strasbourg, 2020.
[10] D. Kessler, B.G. Cour-Palais, Collision Frequency of Artificial Satellites: The Creation of a Debris Belt, 1978 [online] Available at: https://agupubs.onlinelibrary.wiley.com/doi/epdf/10.1029/JA083iA06p02637. (Accessed 5 April 2020).
[11] J. Robinson, Transparancy and confidence-building measures for space security, Space Pol. 37 (3) (August 2015) 134–144.
[12] Department of Homeland Security, Space Weather, 2020 [online] Available at: https://www.ready.gov/space-weather. (Accessed 13 April 2020).
[13] R.C. Carrington, Description of a Singular Appearance Seen in the Sun, September 1, 1895 [online] Available at: https://babel.hathitrust.org/cgi/pt?id=njp.32101081655332&view=1up&seq=351. (Accessed 5 April 2020).
[14] S. Ritter, D. Ratko, S. Halpin, A. Nawal, A. Farias, K. Patel, A. Diggewadi, H. Hill, International and legal issues of a future Carrington event: existing frameworks, shortcomings and recommendations, New Space 8 (1) (2020) 23–30.
[15] B. Unal, P. Lewis, Cybersecurity of Nuclear Weapons Systems, Threats, Vulnerabilities, and Consequences, 2018. Available at: https://www.chathamhouse.org/2018/01/cybersecurity-nuclear-weapons-systems. (Accessed 17 July 2021).
[16] R. Rajagopalan, Electronic and Cyber Warfare in Outer Space, 2019 [online] Available at: https://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf. (Accessed 10 July 2021).
[17] J. Rabkin, J. Yoo, Striking Power: How Cyber, Robots, and Space Weapons Change the Rules of War, Encounter Books, New York, 2017.
[18] M. Moon, The Space Domain and Allied Defence, NATO Report 162 DSCFC 17 E rev.1 Fin, NATO, Brussels, 2017.
[19] W. Akoto, Hackers Could Shut Down Satellites – or Turn Them into Weapons, 2020 [online] Available at: https://theconversation.com/hackers-could-shut-down-satellites-or-turn-them-into-weapons-130932. (Accessed 8 March 2020).
[20] P. Tucker, The NSA Is Studying Satellite Hacking, Defense One, Sep 20. 2019 [online] Available at: https://www.defenseone.com/technology/2019/09/nsa-studying-satellite-hacking/160009/. (Accessed 8 March 2020).
[21] S. Wee, K. Wills, Y. Nishikawa, China denies it is Behind Hacking of U.S. Satellites, Reuters, 31 October 2011 [online] Available at: https://www.reuters.com/article/us-china-us-hacking/china-deniesit-is-behind-hacking-of-u-s-satellites-idUSTRE79U1YI20111031. (Accessed 8 March 2020).
[22] M. Flaherty, J. Samenow, L. Rein, Chinese Hack U.S. Weather Systems, Satellite Network, Washington Post, 12 November 2014 [online] Available at: https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellitenetwork/2014/11/12/bef1206a-68e9-11e4-b053- 65cea7903f2e_story.html?utm_term=.186f9653e25b. (Accessed 8 March 2020).
[23] Holmes, M., The growing risk of a major satellite . In Via Satellite, [online] Available at: http://interactive.satellitetoday.com/the-growing-risk-of-a-major-satellite-cyber-attack/. (Accessed 19 January 2021).
[24] European Commission, Cybersecurity, 2020 [online] Available at: https://ec.europa.eu/digital-single-market/en/cybersecurity. (Accessed 9 February 2021).
[25] McGuinness D. How a transformed Estonia. [online] Available at: https://www.bbc.com/news/39655415#:~:text=156%20people%20were%20injured%2C%20one,unprecedented%20levels%20of%20internet%20traffic. (Accessed 27 January 2021).
[26] Davis,J., Hackers take down the most wired country in Europe. [online] Available at: https://www.wired.com/2007/08/ff-estonia/. (Accessed 27 January 2021).
[27] International Telecommunication Union (ITU) Estonia ranks fifth in the global cybersecurity index. [online] Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/Estonia-ranks-fifth-in-the-global-cybersecurity-index.aspx. (Accessed 27 January 2021).
[28] Greenberg, A. The untold story of NotPetya, the most devastating cyber-attack in history [online] Available at: https://www.wired.com/story/notpetya-cyber-attack-ukraine-russia-code-crashed-the-world/. (Accessed 27 January 2021).
[29] J. Wakefield, Tax Software Blamed for Cyber-Attack Spread, 2017 [online] Available at: https://www.bbc.com/news/technology-40428967. (Accessed 27 January 2021).
[30] Cerulus,L. How Ukraine became a test bed for cyberweaponry [online] Available at: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/. (Accessed 27 January 2021).
[31] The Economist, Ransomware attacks like the one that hit Colonial Pipeline are increasingly common, Graphic detail, 2021, 10 May 2021. [online] Available at: https://www.economist.com/graphic-detail/2021/05/10/ransomware-attacks-like-the-one-that-hit-colonial-pipeline-are-increasingly-common. (Accessed 3 July 2021).
[32] L. Newman, Colonial Pipeline Paid a $5M Ransom and Kept a Vicious Cycle Turning, 2021 [online] Available at: https://www.wired.com/story/colonial-pipeline-ransomware-payment/. (Accessed 3 July 2021).
[33] S. Lynch, FBI Director Wray Urges Companies to Stop Paying Ransoms To Hackers, 2021 [online] Available at: https://www.reuters.com/technology/fbi-director-wray-urges-companies-stop-paying-ransoms-hackers-2021-06-23/. (Accessed 3 July 2021).

[34] BBC News, J. Tidy, Gang Behind Huge Cyber-Attack Demands $70m in Bitcoin, 2021 [online] Available at: https://www.bbc.com/news/technology-57719820. (Accessed 5 July 2021).
[35] Standage,T. (The Economist - the World in 2021), the world in numbers: industries, [Information Technology online] Available at: https://www.economist.com/the-world-in-2021. (Accessed 28 January 2021).
[36] H. Moynihan, The Application Of International Law to State Cyberattacks Sovereignty and Non-Intervention, 2019 [online] Available at: https://www.chathamhouse.org/sites/default/files/publications/research/2019-11-29-Intl-Law-Cyberattacks.pdf. (Accessed 17 July 2021).
[37] United Nations GE PAROS, Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space, 2019 [online] Available at: https://undocs.org/GE-PAROS/2019/WP.1. (Accessed 18 July 2021).
[38] BBC News, Biden Vows US Actions Over Russian Cyber-Attacks, 2021 [online] Available at: https://www.bbc.com/news/world-us-canada-57786302. (Accessed 17 July 2021).
[39] The United States Department of Justice Office of Public Affairs, Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace, Justice News, 2020. Monday 19 October 2020 [online] Available at: https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and. (Accessed 17 July 2021).
[40] X. Wu, China and space security, Space Pol. 33 (2015) 20–28.
[41] P. Martinez, R. Crowther, S. Marchisio, G. Brachet, Criteria for developing and testing Transparency and Confidence-Buiding Measures (TCBMs) for outer space activities, Space Pol. 30 (2014) 91–97.
[42] D. Livingstone, P. Lewis, Space, the Final Frontier for Cybersecurity? Chatham house The Royal Institute of International Affairs, London, 2016.
[43] UK Government, UK Push for Landmark UN Resolution to Agree Responsible Behaviour in Space, 2020 [online] Available at: https://www.gov.uk/government/news/uk-push-for-landmark-un-resolution-to-agree-responsible-behaviour-in-space. (Accessed 5 July 2021).
[44] United Nations General Assembly 75th sess.: 2020-2021, Reducing Space Threats through Norms, Rules And Principles of Responsible Behaviours: Resolution/Adopted by the General Assembly, 2020 [online] Available at: https://digitallibrary.un.org/record/3895440?ln=en. (Accessed 5 July 2021).
[45] ORS, About ORS, see http://ors.csd.disa.mil/ (Accessed 27 July 2020).
[46] Doggrell. L, Operationally Responsive Space, Defense Technical Information Center Compilation Part Notice ADP023958, 2006 [online] Available at: https://apps.dtic.mil/dtic/tr/fulltext/u2/p023958.pdf. (Accessed 22 July 2020).
[47] M. Wall, Converted Missile Launches Military Satellite to Track Spacecraft and Debris, Space.com, August 26, 2017 [online] Available at: https://www.space.com/37959-air-force-launches-ors-5-satellite.html. (Accessed 27 July 2020).
[48] J. Wertz, R. Conger, J. Kulpa, Responsive launch with the scorpius family of LowCost expendable launch vehicle, in: 1st Responsive Space Conference, 1-3 April 2003 Redondo Beach, US-CA, AIAA, Reston, US-VA, 2003.
[49] Bryce, 2019 Global Space Economy, Bryce TechReports, 2020 [online] Available at: https://brycetech.com/reports. (Accessed 10 February 2021).
[50] I. Leveson, The Economic Benefits of GPS, GPSWorld, 1 September 2015 [online] Available at: https://www.gpsworld.com/the-economic-benefits-of-gps/. (Accessed 25 June 2018).
[51] ISU, Without Space, White Paper, ISU, Strasbourg, France, 2019.