IAC-21-E9,2,7,x66298

Space as NATO's Operational Domain: The Case of the Cyber Threats against GNSS

Laetitia Zarkan Cesari[1,1ab]*, Antonio Carlo[1,2a], Nebile Pelin Mantı[1,3a], Lucille Roux[1,4a]
[1] First Author
[a] *Space and Cybersecurity Project Group of the Space Generation Advisory Council (SGAC)*
[b] *laetitiazarkan@gmail.com*
* Corresponding Author

Abstract

In the last decades, modern society has become growingly dependent on new technological and digital domains. In this view, the North Atlantic Treaty Organization (NATO) identified and defined two areas, cyber and space, as operational domains alongside land, sea and air. Such development reflects the threat landscape that stems from a society more dependent on technological solutions, where space and cyber may have a prominent role in future conflicts. Currently NATO is developing rules on engagement for cyber-attacks and attacks against space assets. At the same time, NATO explores the potential of space capabilities during a conflict and prepares for preventing adversaries from doing the same, which is critical to the success of military operations. A hostile act carried out against a satellite system could have widespread consequences. If there is a `strike' in cyberspace, it would be most likely against a strategic system providing an important service used during conflicts. In this paper, Global Navigation Satellite System (GNSS) is identified as the most critical space system that could be subject to a cyber threat.

NATO does not have its own space capabilities and relies on the members of the alliance to provide access and information. Given the growing importance of space technology and of its protection against cyber risks, NATO's role with regard to national divergent interests shall be analysed. Within its framework, there is still more to be done in terms of coordinating efforts and designing resilience strategies against future threats. Against this background, NATO's response to cyber threats against space systems will be examined using as a reference NATO's conduct in other operational domains.

The paper will examine what legal and policy repercussions could follow from the loss of GNSS signal, whether for a limited time or a prolonged period. It will conclude that the recognition of space and cyber as operational domains is a step toward preparing NATO for threats and possible competitors. It will also suggest strategies for building defences for the intersection of these domains, taking into account the provisions of the North Atlantic Treaty and other relevant instruments of the Organization.

Keywords: GNSS, cyber-attack, NATO

1. Introduction

The advances within the space sector creates new opportunities and challenges. It has become an area essential to NATO's deterrence and defence. "Space provides a number of critical military functions in peace time, as well as in crisis and conflict. NATO is increasingly reliant on space to navigate and track forces, to detect missile launches and to ensure effective command and control. For example, satellite imagery can play a significant role in NATO's decision-making process" [1]. "Out half of the currently deployed active satellites are owned by NATO Allies - NATO relies on space to navigate and track forces, to have robust communication, to detect missile launch and to ensure effective command and control. each nation responsible for defending its space assets itself" [2].

"NATO's missions and operations are conducted in the air, land, cyber and maritime domains. Space-based architecture is fundamental to the provision of data and services in each of these contexts. While the Alliance's reliance on Space-based Data, Products, and Services (DPS) grows, members face a more contested Space domain with new kinetic and non-kinetic threats. The critical dependency on space has resulted in new cyber risks that disproportionately affect mission assurance. Investing in mitigation measures and in the resilience of space systems for the military is key to achieving protection in all domains" [3]. With the multiplication of cyber hostile operations targeting space systems and the increasing reliance on said space systems, the nexus between space and cyber is becoming one of pressing importance for collective security.

2. Background & Current Practices

NATO's founding Washington Treaty [4] defines the Alliance's mission and mandate as "defensive". It means that any attack against one Ally could lead to the invocation of Article 5 of the North Atlantic Treaty [5]. NATO's current Strategic Concept sets out the three core tasks as "collective defence, crisis management, and

cooperative security" [6]. To fulfil these tasks and fight against new threats, the heads of State and government of 30 Allied countries [5] reaffirmed this year their defensive mission and mandate against multifaceted threats and systematic competition. Allied countries also underlined the need for resilience, as a national responsibility and collective commitment [7].

As part of the Alliance, NATO Allies commit to procure equipment and software to be integrated into their national defence architecture, which becomes part of the overall NATO capability [3].

Pursuant to Rule 2 of the Oslo Manual on Selected Topics of Law Armed Conflicts, a collective work which restates the current law of armed conflict regarding hostilities in a diverse range of contexts, Outer Space operations are governed by international law, including the Charter of the United Nations and the applicable principles and rules of the Law of Armed Conflict (LOAC) [8].

This Manual restates the provisions of the Outer Space Treaty, a text considered as the basis of international space law, of which Article III provides that space activities must be carried on "in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding" [9].

Considering the recent public declarations that space is an operational domain, the question of the law applicable to the use of space technologies, among which Global Navigation Satellite System (GNSS), and to the protection of space assets used for military operations, has been thrusted at the forefront of the international discussions.

2.1 Operational Domain vs Warfighting Domain

NATO does not have an official definition of a domain, nor a set of criteria for what constitutes a domain. The term is defined in the dictionary as "a territory over which rule or control is exercised", and as "a sphere of activity, interest, or function" [10]. In international humanitarian law, domain is an area in, from, and through which military operations create intended effects [11]. According to researchers, such a declaration is a recognition of "the role of space in military operations and the importance of space for national security" [12].

Since 2012, as a human-built domain, cyberspace has been accepted as an operational domain [13]. During Wales Summit in September 4-5, 2014, NATO acknowledged that international law applies to cyberspace, and that cyberspace is part of NATO's core task of collective defence, and The Enhanced Cyber Defence Policy was endorsed in Wales Summit Declaration [14] in 2014 and updated in 2018. On 14 June 2016, Allied defence ministers agreed to recognise cyberspace as an operational domain at the NATO Summit in Warsaw in July, without changing NATO's mission or mandate, which is defensive [4].

NATO uses space for a wide range of activities, from communication (Satellite Communications, SATCOM), intelligence-gathering (Intelligence, Surveillance, Reconnaissance, ISR) and the focus of this article: navigation, to tracking forces around the globe (Positioning, Navigation & Timing (PNT)) and detecting missile launches (Deterrence).

Alliance's all modern military engagements rely more and more on space-based assets, yet NATO does not have its own space assets as it benefits from the Allies capabilities. Since more than half of the 3,000 active satellites orbiting Earth belong to NATO members or companies based on their territory [15], NATO will continue to rely on national space assets of members [16].

Following the London Summit and declaration of space as an operational domain by North Atlantic Council in London 3-4 December 2019, NATO formally declared space as "an operational domain", along with air, land, sea and cyberspace, but "without weaponization" [17] in order to avoid an arms race, and to limit the use of space only to national security, as recognised by the Alliance. And then, NATO recalled the utter importance of conducting space activities in compliance with international law [5].

The strategic importance of Space drove NATO in October 2020 to establish a NATO Space Centre at Allied Air Command in Ramstein, Germany [18].

US Chief of Space Operations, General John W. "Jay" Raymond defined space as "a warfighting[1] domain" early in August 2019, before the establishment of the US Space Force, on the Pentagon brief. "Although space is a warfighting domain, our goal is actually to deter a conflict from extending into space; the best way I know how to do that is to be prepared to fight and win if deterrence were to fail"[2], he affirmed. Following the establishment of the US Space Force on October 28, 2020, during a press conference, added that "it is clear today that space is a warfighting domain just like air, land and sea", and he "couldn't have said that five or six years ago".

The preference of the terms reflects an important change (a paradigm shift in thinking), as there is an important difference between taking space as an operational domain and as a warfighting domain. (Also, NATO and

[1] Warfighting is defined as "fighting between the armed forces of countries that are at war". Available at: https://www.macmillandictionary.com/dictionary/british/warfighting

[2] The first 'space war' or 'space enabled war' was the First Gulf War, since the early 90s, space has been used for GPS, PGMs, satellite communications, etc. to enable war on Earth, during which space was not officially defined as a warfighting domain.

US Military do not understand and define "domain" the same way.)

The NATO doctrine takes the concept of "domain" as different dimensions of an "operation environment", including its land, air/space, maritime dimensions, as well as the Political, Military, Economic, Social, Infrastructure, and Information Systems (PMESII), systems of main adversaries [19]. Operational domain, in this sense, covers "maintaining situational awareness and reliable access to space services that are critical to the success of NATO's operations, missions and activities for the objectives of the Alliance".

The use/choice of the term "warfighting domain" by US officials, on the other hand, might signal a change, that "an armed conflict is inevitable". Professor Michael Schmitt [20] underlined in 2018, that the use of space today is more than reliance on space assets for the success in the armed conflicts, it is winning a war that extends to space. This declaration is one of the consequences of the militarization of space, which means the nations are in a process of becoming ready for (an armed) conflict or war in Space. Many NATO Allies, testing their readiness with wargames[3]; such as the US since 2012 with Schriever Wargames[4] emulated a national NATO operation with reliance on space-based capabilities provided by member nations, and training NATO Subject Matter Experts (SMEs) [21]. France in lead with AsterX Wargame in March 2021 together with the US, Germany, Italy outlines the importance for European countries to focus, first on the assessment of satellite protection and surveillance capabilities. On one hand, Russia and China have been developing counter-space capabilities and testing them since 2007.

Concerning the qualification of cyberspace as an operational or warfighting domain for NATO and Allied states. According to NATO website, cyberspace is a domain in, from, and through which military operations create effects [22].

This dimension of military space operations represents the primary linkage to the other warfighting domains and enables command, control, and exploit space capabilities through a physical and logical architecture that collects, transmits, and processes data around the world and across the domain.

2.2 NATO in Cyber, Rules of Engagement

One of the most important questions remains as to reliance on the NATO Allies assets for future operations, and how collective priorities will be balanced with/against those of national interests?

Cyber threats to Alliance security are becoming more frequent, complex, destructive, and coercive [23]. NATO has established a roadmap to Cyberspace as an operational domain approach, and the Allies have taken important steps in cyber defence over the past decade. In 2018, they agreed on how to integrate sovereign cyber effects, provided voluntarily by Allies, into Alliance operations and missions, as well as to stand up the initial Cyberspace Operations Centre, with activities along the following lines of effort: training, capability development, organizational constructs, operational planning, exercises and strategic communications, and reinforced the Alliance's hybrid and cyber defences by establishing Counter-Hybrid Support Teams and a Cyberspace Operations Centre. However, what is NATO going to do in order to address the complex and evolving challenges in cyberspace?

The 'deterrence' emphasis in connection with cyberspace is significant and can be considered as another step towards the acceptance of offensive cyber capabilities as part of NATO's collective defence policy. From national to collective operations, whether defensive or offensive, the integration of national cyber capabilities or offensive cyber capabilities into allied operations and missions, also requires updating allied baseline requirements for national and allied effectivity and resilience, including energy, transport, and communications, as well as regulating the impact of 5G and other new technologies.

Among many steps taken by NATO, such as investments to NATO Space Centre, 1.4 billion Euros of investment in new technologies in areas ranging from cybersecurity to surveillance and reconnaissance, and sharing the information gathered by remotely piloted platforms[5], one of the largest [6] in this regard, has planned for the acquisition of the satellite capacity to provide more secure and quick communication for forces in different combat environments.

[3] Wargaming plays an important role for the modern military, to know better the geography and relevant terms of an environment, as it provides an analytic approach to real life crisis, and helps to simulate aspects of warfare at the tactical, operational, or strategic level, provides ground to examine adopted warfighting concepts, train and educate commanders, personnel, and analysts, enables to explore scenarios, and assess how force planning and posture choices will affect future campaign outcomes. Jonathan Cham, Katherine Pfrommer, Wargaming, RAND, 2021.

[4] Schriever Wargames first initiated in 2001, under US Air Force Space Command, to assemble a military coalition of spacefaring nations to rival that of Operation Enduring Freedom or the Western Bloc.

[5] Earlier in 2019, SACEUR declared a major milestone programme, namely The Joint Enterprise for Intelligence, Surveillance and Reconnaissance, which is NATO's fleet of new Alliance Ground Surveillance aircraft initially operationally ready to conduct missions, with a reset on EMS/EW.

[6] This sum is pronounced as over 1 billion euros worth to acquire new satellite capacity in 2020–2034.

Cyber capabilities are extremely relevant when they are integrated with Air and Space capabilities, in multi- or all-domain operations, as the skilful coordination and management of resources are assured in and through Cyberspace [24]

NATO's 2021 JAPCC Conference theme is determined as 'Delivering NATO Air & Space Power at the Speed of Relevance', considering the actual execution of Air and Space operations, the integration and coordination of resources of/in multiple domains in time and space is essential for mission success, so securing the cyber-network across these domains, which this coordination takes place, is paramount. In contemporary military operations, superiority is not permanent, and will be challenged by multiple means, multiple times, by various vectors including technology, in multi- or all-domain operations, while Air and Space capabilities are integrated with cyberspace and brought to bear against an adversary. The digitally interconnected systems establish larger lethal systems, and a myriad of attack surfaces with varying degrees of vulnerability to attack in and through cyberspace, which introduces greater risk to Air and Space operations, and air and space supported missions [24].

2.3 NATO in Space: NATO's Strategy. The Use of GNSS, etc. - Difference in Users and Providers

The 1949 North Atlantic Treaty does not acknowledge Outer Space within its articles, the Treaty's wording makes it unclear whether NATO's 'collective self-defence'[7] umbrella, provided through Article 5, would apply to the space operational domain; neither explicitly denies the possibility for parties to carry out operations in Outer Space.

NATO leaders have identified Space technologies as one of seven critical, emerging, and disruptive technologies essential for the Alliance to maintain a technological edge [25]. In order to adapt and meet rapidly evolving space and counter-space threats, on June 27, 2019, at the Defence Ministers' meeting, Allies adopted NATO's Space Policy [26] and in November 2019, the North Atlantic Treaty Organization (NATO) declared "outer space" to be its fifth operational domain [27] but not a warfighting domain. In September 2020, decided to create an 'Air and Space Operations Centre'. A month later, NATO created its first-ever Space Centre in Germany and in 2021 it was decided that France would host the new NATO Centre for Excellence in military space.

The first challenge for NATO in Outer Space is regulatory, while the increasingly congested, contested, commercial, and competitive nature of Space operations intensifies the need for legal clarity and harmonization, the development of national space law frameworks are at a different pace. The lack of clarity weakens the alliances options for deterrence, therefore, as Secretary General Stoltenberg highlighted [28] build on previous cyber-attack declarations to issue a formal declaration stating the readiness to counter attacks on Allied Space assets, including an explanation of which assets fall within the scope of the Treaty [29]. As a result, following the collective commitment under Article 3 of the North Atlantic Treaty, to reduce vulnerabilities and ensure Allied militaries can effectively operate in peace, crisis and conflict, to strengthen interoperability and understand vulnerabilities,

While the institutional development is rapid, member states' legal development at different pace and adoption of different standards, can lead to the progressive dismantling of regulatory standards or, as NATO Officials used, to a 'race to the bottom', which could compromise the interoperability of the Space legal frameworks of the member states, and reduce the collective value of space assets and negatively impacts NATO's Space power projection [29]. To this end, one of NATO's space policy priorities is to foster enhanced interoperability by fostering a common legal Space doctrine based on agreements on fundamental mechanisms, international standards, or norms of behaviour, in which Allies can collaborate using operational assets and national policies or frameworks.

"NATO does not own satellites, but owns and operates terrestrial elements, such as satellite communications anchor stations and terminals. It requests access to products and services of member states – such as space weather reports and satellite overflight reports provided via satellite reconnaissance advance notice systems – but does not have direct access to satellites: it is up to individual NATO member states to determine whether they allow access".

Qualified as a civilian infrastructure, GNSS is a worldwide civilian infrastructure and targeting of GNSS would have wide-ranging repercussions for both civilians and military. The legal aspects associated with hostile cyber operations against GNSS concern international telecommunications law, namely the ITU body of agreements and regulations on the use of radio frequencies. The navigation satellites used by the military are vital for NATO communications and transportation networks, especially when navigating in maritime areas without terrestrial orientation.

2.4 Legal conduct in operational domains

Space power is uniquely infrastructural and connected to Earth [30]. As highlighted in the Brussels Summit in 2019, the NATO Allies are committed to international

[7] In a pragmatic approach, the NATO Treaty regulates 'collective self-defense' in Article 5, if an "armed attack" occurs, and as the prerequisite to activate Article 5, Article 6 defines an armed attack.

law and Alliance's strategic, tactical, and policy success in space operations relies on the 'sensitivity to the legal rules of the game'. In response to cyberattacks that infringes international law (including use of force), States can take countermeasures designed to:

i. protect their interests and ensure they are respected; and
ii. induce the State responsible to comply with its obligations[8].

Under the Tallinn Manual, hostilities, including those involving cyber operations, in, though, or from outer space, which cross the threshold of armed conflict According to Rules 82–83, the law of armed conflict will govern them. If the 'hostile' space operations are considered as an "armed attack" [31], under Article 51 [32] of the UN Charter and customary international law, this entitles the victim State to respond individually with armed force in self-defence or ask the Alliance (or individually any allied State) for assistance in collective self-defence. The 2019 communiqué is remarkable in this regard, as it confirmed in the first place that "attacks to, from, or within space… could lead to the invocation of Article 5" of the North Atlantic Treaty [4].

Under Article 5, upon the request of the victim State, the North Atlantic Council takes a decision and NATO can plan, equip, and train for forcible responses to hostile space operations, and all parties' actions would be subject to the prohibitions, limitations, and requirements of International Humanitarian Law [11].

Self-defence in response to an armed attack carried out in cyberspace might involve digital or conventional means in compliance with the principles of necessity and proportionality[9].

A State's cyber operation conducted in self-defence as to Rule 71, does not violate this Rule and cannot be an excuse for violations of the law of armed conflict when the exchange between the States concerned qualifies as an armed conflict.

Therefore, LOAC prohibition of conducting cyber-attacks against civilian objects (Rule 99) would equally apply to cyber-attacks against civilian space objects that are not being used for military purposes (and therefore do not qualify as military objectives).

The main problem, in this context, would arise from the widespread phenomenon of dual use satellites and other cyber infrastructure in outer space.

At the 2021 Brussels Summit, NATO recognised that "attacks to, from or within space present a clear challenge to the security of the Alliance". Therefore, an attack on one of the Allied infrastructures could lead to the invocation of Article 5 of the North Atlantic Treaty.

3. Peacekeeping vs War

NATO decided to offer its support for peacekeeping operations under the responsibility of the UN Security Council in the course of the Brussels Ministerial Meeting of 17 December 1992 [33]. While peacekeeping for NATO would consist of use of satellites, operated under the aegis of the international community which would be instrumental in performing one or more of the functions such as verifying international treaties, especially arms control and disarmament treaties; monitoring conflicts or crises; supporting peace-keeping operations, such as those performed by the United Nations; managing natural catastrophes. Therefore, the Alliance depends on member states' assets for reliable, neutral information on security-threatening or security-enhancing developments anywhere on the planet. NATO's approach to the protection of civilians is based on legal, moral, and political imperatives [34]. The protection of civilians, where applicable, includes a range of activities up to and including the use of force, as appropriate, to prevent, deter, pre-empt, and respond to situations in which civilians suffer physical violence or are under threat of physical violence [35].

At the Brussels Summit, the Allies stressed that NATO's space policy "will remain fully in line with international law". The communiqué confirmed that "attacks on, from or within space ... could lead to Article 5 invoking" of the North Atlantic Treaty. In other words, in accordance with Article 51 of the Charter of the United Nations and customary law, space operations can be regarded as "armed attacks", giving the injured country the right to use its own force to respond and seek assistance from alliances (or individual countries) in collective defence.

A cyber operation against space assets, whether offensive or defensive, could reasonably be expected to cause

[8] Article 49, §1 of the Draft Articles on the Responsibility of States for Internationally Wrongful Acts, International Law Commission (ILC).

[9] Military and Paramilitary activities in and against Nicaragua, Nicaragua v United States of America, judgment, ICJ Reports 1986, §194 and §282 states that "The Parties also agree in holding that whether the response to the attack is lawful depends on observance of the criteria of the necessity and the proportionality of the measures taken in self-defence. […] The measures must not merely be such as to tend to protect the essential security interests of the party taking them, but must be 'necessary' for that purpose"; and Advisory opinion on the Legality of the Threat or Use of Nuclear Weapons, ICJ Reports 1996, § 41 states that "There is a specific rule […] well established in customary international law" whereby "self-defence would warrant only measures which are proportional to the armed attack and necessary to respond to it".
Schmitt, Michael N., 'Attack' as a Term of Art in International Law: The Cyber Operations Context (September 7, 2012). Proceedings of the 4th International Conference on Cyber Conflict 283-293 (Christian Czosseck, Rain Ottis & Katharina Ziolkowski eds., 2012). Available at: https://ssrn.com/abstract=2184833

injury or death to persons or damage or destruction of objects under IHL. The first crucial point is defining "damage" in the digital world, and Tallinn experts agreed that damage is not limited to physical damage, loss of functionality of an object can also constitute "damage"[10]. In this case, a cyber operation making a civilian network dysfunctional would violate prohibition on targeting directly civilian persons and objects and will be covered by IHL. In such cases, IHL can be applied, if one can characterize a cyber operation as military operations if there is (a) warfare proper (the conduct of military operations within the framework of armed conflict), and (b) "operations other than war", which means operations related to conflict, but outside the framework of armed conflict [36].

NATO implements a different mindset; while some are providing equipment - the other nations must coordinate their actions to protect critical infrastructure. Space assets can be used for military purposes. The main difference may arise where there might be a different definition of what is civilian and what is not. For members who are party to the Geneva Conventions and Protocols, within NATO, they should be compliant to these as a common ground. Standards like STANAG 2449 [37] are only at the minimum, the threshold of compliance is very low, while the US influence is very significant; under the Trump Administration the SPD-7 was published, for maintaining the lead responsibility for any cooperation for access to or information to GPS services. Means that the US is pushing for more influence with their allies.

Along with the new space technologies, the mission variability also increased, such as space transport, space tourism, asteroid mining, lunar operations, and missions to Mars and beyond… The commercialization of space heightens cybersecurity concerns. An attack in outer space could have devastating consequences on Earth, and existing treaties do not yet fully recognize the consequences of space attacks. International law must define the legal framework for networks of linked devices operated in/for these new space missions.

Although it is not possible to give an exhaustive list, whether legal, civil, or military, practitioners must take into consideration the circumstances prevailing at the time of the operation, the origin of the operation and the nature of the instigator/actor (military or not), as well as the extent of intrusion, the actual or intended effects of the operation or the nature of the intended target.

United Nations Charter is based on the principles of the "sovereign equality of States", the "settlement of international disputes by peaceful means" and the requirement for States to "refrain in their international relations from the threat or use of force against the territorial integrity or political independence of another State" or "in any other manner inconsistent with the purposes of the United Nations"[11].

Under international law, a cyber hostile operation is not unlawful per se, but can become so where a cyber "operation or its effects" entail violations of international law. Accordingly, "the extent of the intrusion or its effects", may violate the principles of sovereignty, non-intervention or even the prohibition of the threat or use of force. Keeping in mind the possibility that a cyber operation without physical effects can also be characterised as a use of force.

The series of cyberattacks, which do not meet the threshold of an armed attack individually, could be categorised as an armed attack, in case the accumulation of their effects reaches a certain/sufficient threshold of gravity [38], or they can be taken as "armed attack" when they are carried out as a part of operations in the physical sphere which constitute an armed attack, and where such cyber-attacks are coordinated and stem "from the same entity" or "from different entities acting in concert".

For the assessment of "armed attack" or "gravity", Tallinn Manual 2.0 suggests that operations are judged by their scale and effects, rather than simply the nature (destructive or injurious) of the consequences (Tallinn Manual 2.0, Rule 69) This approach is adopted by NATO states, but not by some non-NATO states (e.g., Australia).

Until 2018, cybersecurity of space assets has not been a priority in government and private-sector space endeavours. One leading analysis by Chatham House even asserted that cybersecurity discussions often overlook space activities' vulnerability to cyberattacks. Neither the UN Governmental Group of Experts (GGE) on outer space [39] nor the UN GGE on cyberspace [40] addressed the convergence of their respective agendas.

On the other hand, France in 2019, considered penetrating military systems in order to compromise French defence capabilities, or financing or even training

[10] M. N. Schmitt, Tallinn Manual on the International Law Applicable to Cyber Warfare (Cambridge University Press: Cambridge, 2013), Rule 30(11). The notion of damage applies not only to the targeted computer (first order of effect), but also to the impact on any potential installation it might service or control (second order of effect) as well as the impact on the people affected by the shutdown of the services of that installation (third order of effect). Boothby, W. H., 'Methods and means of cyber warfare', International Law Studies, vol. 89 (2013), p. 389.

[11] 1945 United Nations Charter, Article 2, para. 4: "All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations". There are only three exceptions to the prohibition of the use of force: self-defence in the event of armed aggression (Article 51 of the United Nations Charter), the use of force authorised by the United Nations Security Council under Chapter VII, and the consent of the State on whose territory the operation takes place.

individuals to carry out cyberattacks against France, as uses of force. While the Netherlands considered in 2019, during the use of force threshold discussions that "a cyber operation with a very serious financial or economic impact may qualify as the use of force" [41].
Cyber practice Toolkit suggests, as of 2020, there is limited State practice supporting the claim that the meaning of "force" has evolved and include non-destructive cyber operations against critical national infrastructure [42] and no victim State of such an operation of this kind has ever suggested that the operation would have amounted to use of force [43] Interpretation of essential notions has also to be taken into consideration. The disagreements in the U.N. Group of Governmental Experts (GGE) sessions in 2019 as to the binding force of the principle of "due diligence", prevented the group from securing agreement on this critical issue and deploying secure communication infrastructures. While the "due diligence" principle requires States to take feasible measures to stop hostile cyber operations from or through their territory that have serious adverse consequences for the international legal rights of other States, NATO members are divided over whether due diligence is a mandatory rule of international law or only a "voluntary, non-binding rule of responsible state behaviour", that is, behaviour in which responsible members of the international community should participate. General John W. Raymond of the U.S. Space Force recognizes this potential for the future development of international norms of responsible behaviour in the exploration and use of the space environment, NATO Allies have to develop shared understandings and expectations about how international law applies to space operations and on how to respond hostile operations undertaken by peer and near-peer competitors.

4. GNSS

The Global Positioning System was originally designed as a military system, to meet tactical and strategic needs on the battlefield, during the Cold War Era. The term traditionally refers to the North American global positioning system, or satellite positioning system, while GNSS refers to the International Multi-Constellation Satellite System. Therefore, GNSS as an umbrella term typically includes GPS, GLONASS, Baidu, Galileo, and any other constellation system.

4.1 Importance of GNSS

GNSS and GPS work together, however the GNSS-compatible equipment can use navigational satellites from other networks beyond the GPS system, which is the main difference from GPS, and more satellites means increased receiver accuracy and reliability.
The GNSS can be targeted by cyberattacks via the command connection or ground station, since an unencrypted command link can expose the satellite's capabilities to an opponent, or a ground station could be hacked directly, allowing the ground station to influence satellite control or data.
The ITU, while recognizing that "Member States retain their entire freedom with regard to military radio installations" [44] these installations must, so far as possible, take measures to prevent harmful interference [45]. Therefore, when assessing the interference risks associated with conflict zones or planning military exercises, ITU invites Member States to consider that the use of satellite-based systems can potentially be impacted beyond that zone, and therefore, an enhanced civil-military coordination is required.
NATO's ballistic missile defence capability is being built around a command-and-control system that enables five key functions: planning, monitoring, information-sharing, interception and consequence management[12]. The security of the system relies on three key elements, confidentiality, integrity and availability. industrial security is paramount (inc also supply chains)" [2].

4.2 Potential impacts of cyber attack

The consequences of cyber-attacks on space missions are aggravated because of component satellites' augmented connectivity and use of Internet of Things (IoT) devices in contemporary space systems. The potential impacts of an attack on a communication satellite can endanger national security by generating widespread disruptions to communication channels, not only national level, but also across widespread geographies, cross countries, and cause panic.
The attacker can infiltrate the network without being detected and remain undetected.
Cyber threats may target different components of a space mission: the ground segment, the space segment, and the link segment. The vulnerabilities stem from the ground segments; mostly generated from network components and the receivers (which receive the data from the satellite). The threats may also target hardware of satellites in the supply chain, and compromise ground units at a later stage [46].
"Cyber vulnerabilities undermine confidence in the performance of strategic systems. As a result, rising uncertainty in information and analysis continues to impact the credibility of deterrence and strategic stability.

[12] Each of these functions may use satellite-based positioning, navigation and timing, intelligence, and communications services to some degree. Significantly, the monitoring function incorporates space-based early warning. Once detected the missiles are tracked using sea and land-based radar computer systems such as aegis and their interception is arranged through sophisticated command control. due to the nature of the task, time and accuracy are of the absolute essence.

Loss of trust in technology also has implications for determining the source of a malicious attack (attribution), strategic calculus in crisis decision-making and may increase the risk of misperception" [47]

4.3 Cyber Threats Against GNSS

Ground stations - how can we prevent threats? Preventive method and time-based method. Previous attack on ISS.

GNSS are specifically vulnerable to hostile cyber operations because of the very low power of their signals and services and constitute potential primary targets in future wars because of their importance not only for military operations, but also for critical national infrastructure and key economic sectors. Unlike physical attacks they are not likely to cause major damages to the satellite navigation system. Recent cyber operations against GNSS were jamming and spoofing [48] although other types of attacks such as hacking or eavesdropping of communications satellite systems, are also technically possible.

In 2018, during NATO Trident Juncture, NATO's biggest military maneuverer since the end of the Cold War [49] took place in southern and central Norway, plus the North Atlantic and Baltic Sea between October 25 and November 7. NATO officials confirmed the disruption on November 11 [50].

Cybersecurity for satellite Ground Systems has been neglected. With the increasing number of small satellites and a global network of ground stations needed to provide low latency for data getting between low earth orbit and users, the threat surface for cyberattacks has grown significantly.

We are in a phase in which we need to mitigate the risks by simplifying the necessary controls, using time-based methods for analysing controls and preventive cybersecurity mechanisms on new systems in order to provide data assurance.

The targeting of space ground systems increased over the last years with highly sophisticated attacks occurring over the last couple of years. Many attacks took place for different reasons, like the non-update of certain vital software to the operating system and that was the case of the International Space Station computers.

In 2008, hackers infiltrated the Johnson Space Center's mission control computer network and were able to have the mission control network upload a malicious Trojan horse access program onto computers on the ISS disrupting on-board communications [51]. In March 2011, the theft of an unencrypted NASA laptop resulted in the loss of algorithms used to command and control the International Space Station [52].

Another cybersecurity issue concerns the vulnerabilities in GPS receivers' software which rendered GPS's precision timing invalid. Here instead of spoofing or jamming the GPS signal, the actors attack the inherent weaknesses of GPS's design to disrupt the timing.

Most of the existing cybersecurity risk management policies emphasize on identifying potential cybersecurity issues in the early phase of acquisition, in a way the security of these systems is built into the ground systems right before the deployment.

The first step in a good cybersecurity strategy is having a risk management framework to determine what assets are most attractive to hackers and how they should be protected. This means considering all the existing assets (physical and virtual) and the cost associated with the access to these assets by the hacker. We need to consider the type of data that we have in transit like the commands and control communications, live monitoring information, satellite data that will be transferred and the data at rest like databases with satellite information, secured APIs etc.

Among the existing effective frameworks, we mention the Cybersecurity Maturity Model Certification (CMMC) [53] that is a program initiated by the United States Department of Defense (DoD) in order to measure their defence contractors' capabilities, readiness, and sophistication in the area of cybersecurity.

The CMMC have different stages of security maturity:

1. Scanning - This is the first step that a corporation thinking about cybersecurity will have;
2. Managed Assessment and Compliance;
3. Formalized Analysis and Prioritization; and
4. Attack Focused Management ending with Stage Optimization

While existing frameworks provide current guidance on cybersecurity, it's important to monitor for any recommended changes on a regular basis.

Many security control models only address the presence of controls first and do not quantify what those controls provide. The assessment of risk in these models remains qualitative and the risk in these models becomes a subjective measurement.

The Time-Based Security method develops the idea of the evaluation of every security measure a system puts in place using a simple mathematical formula for the:

$$Protection\ Time > Detection\ Time + Response\ Time$$

Protection Time is the time a security measure will provide before it becomes compromised or disrupted. Detection Time is the time it takes for the people controlling the system to find out that a compromise occurred. Response Time is the time it takes those people controlling the system to act accordingly. As a result, protection measures from every security process should allocate more protection time than it takes for the system managers to detect and respond to the potential attack.

This model provides a method for evaluating successive multiple controls. If the satellite control console is the target, then each successive control preventing access to it is judged. A high-level example could test the time it

takes attackers to: (1) access to the base network, (2) access to the satellite control network, and finally, (3) access to the console. Commanders then can make true risk-based decisions on whether they can afford additional protections. The major issue of a quantitative time-based model becomes the requirement for granular testing of every security control on an existing system.

The time-based method is applied to new systems, but the selection of security controls becomes a difficult process if the system designers do not consider security at the outset of the design. The selection of security controls in the time-based model may overwhelm system designers. Without an idea of what to protect in a new or modernized ground system, the quantitative model only provides best guesses. Consequently, the quantitative models work best in existing systems.

Another model for risk-based evaluation of space ground systems uses a preventative mission assurance model based on redefining cyberspace as anything processing a signal and then using the six steps of the data lifecycle: generation, processing, storage, communication, consumption, and destruction in evaluating the risk to the system. Unlike the other models that consider the detection and usually the threat vector, this preventive model focuses specifically on the vulnerability [51]

Generally, if we can build a system without vulnerabilities of the operating system then we can assure security. This preventative model requires the re-engineering of communication channels. It does not provide adaptive methods for dealing with existing cyber security channels as those found in existing space systems. In the future, this model will be extremely considered for the modernization and re-engineering of the Air Force Satellite Control Network (AFSCN) ground station network architecture coordinating communications to more than 100 satellites via nine ground stations positioned around the globe.

Threat elements release new risks of attacks daily, so security operations should be adapted in a sustainable way. It is crucial to consider risk models to assess the strength of existing controls against the threats addressing most potential security vulnerabilities. Having an established framework that will react fast and effectively is mandatory at this stage.

Quantum technologies bring potential new capabilities, to develop parameters of threats, solve the algorithms behind encryption keys that protect our data and the Internet's infrastructure and transform cybersecurity.

5. Recommendation

NATO has to review and renew its strategies for building defences by policy development and raising awareness against new and evolving threats, to protect space-based technologies that supplement lost capabilities and negate adversarial interference with space systems.

5.1 Strategies for building defences for the intersection of space & cyber domains, considering the provisions of the North Atlantic Treaty and other relevant instruments of the Organization

NATO relies on its Allied capabilities; therefore, it is essential to have a unique coordinate system to respond during a crisis. The already existing exercises, such as the Crisis Management Exercise (CMX) which focus on cyber, and resilience should be implemented with space assets. This internal and partner consultation and decision-making procedures at the strategic political-military level would help to strengthen the alliance response and resilience. Therefore, NATO has to operate with a renewed focus on improving proficiency in Allied Cyberspace and Electromagnetic Spectrum Operations, by building awareness, developing policies and strategies, acquiring new capabilities, working with industry and academia, and training people to become experts.

Building defence is possible by “raising awareness” throughout the NATO systems, and by creation of regulation through NATO security framework , in a standardized and collective way which require a proactive effort to prevent, detect and prepare forces to respond to incidents, by developing guidelines, resources, and working groups focusing on emerging technologies to protect the space assets, and test coherency of the rules and their application by raising preparedness, building blocks between law and policy requirements for collective defence.

The traditional policy creation mechanisms are based on multilateralism. States and most of the traditional international organizations struggle to adapt themselves to evolving realities of the new technologies and their applications and implications in new domains, such as cyber and space. Another aspect is to keep the will and interests of member states alive for policy development. This requires NATO to revise and update/adapt its mechanisms, in a way to support a clear-eyed, inclusive policy development, to overcome siloed or single domain-based approaches, to manoeuvre and react in the extremely complex environments.

As a military-security organization, and as to its foundational concerns, unlike UN, NATO cannot represent an open forum for the intellectual construction, however, can support and benefit from the effective participation of the commercial actors, which own operate and manage these new domains, and can assess and adapt these new policies created to remain at the speed of relevance, as highlighted in JAPCC 2021 meeting this year.

5.2 Building blocks between space law (the lex specialis) and cyber policies and standards

While rivalry in space, considering Chinese and Russian initiatives, is increasing, the Allies have not agreed on a joint space doctrine, to provide principles of how operations should be planned, prepared, commanded, conducted, sustained, terminated, and assessed, but confined with a policy [54] to direct and assign tasks and prescribe the desired capabilities. Although the initial intention of NATO was not militarizing space, as approved on June 27, 2019, NATO adopted a new space policy to provide guidance for opportunities and challenges as to information sharing and increasing interoperability and recognise space as a domain of warfare during the London summit at the end of 2019 [55]. Therefore, the first step would be to consider adversaries' counter space capabilities, from cyber operations to anti-satellite missiles. Then, focusing on the design, principles and vulnerabilities of the space-based assets is of the top priority. This also requires more focus on the development of the legal framework. As to cyber-attacks on a space system, collective self-defence as to Article 5 grounds would be possible if the attack will have kinetic consequences.

In case of the kinetic consequences that are creating space debris, considering Article 35 of Additional Protocol I to the Geneva Conventions of 12 August 1949, this would constitute "the violation of the responsibility not to cause widespread, long-term and severe damage to the natural environment".

One of the important questions raised is targeting dual-use assets and application of IHL and international law rules. In case a dual use asset is targeted by a cyber-attack, this would be counted as a military objective and would be subject to the rule of proportionality and parties would be obliged to take precautions in attack as well as comply with the principle of distinction (civilians-combatants-civil and military objects).

References

[1] J. Camille Grand, Patrick Turner, Space - NATO's Newest operating Domain, in NITECH Magazine, Issue 4, December 2020. Available at: https://issuu.com/globalmediapartners/docs/nitech_issue_04_december_2020?fr=sNWYwOTIzODkzMTY

[2] Robert Kroeger, LTC Henry Heren, Laurent Smith, Cyber security for space systems, in NITECH Magazine, Issue 4, December 2020. Available at: https://issuu.com/globalmediapartners/docs/nitech_issue_04_december_2020?fr=sNWYwOTIzODkzMTY

[3] B. Ünal, Cybersecurity of NATO's Space-based Strategic Assets, International Security Department, Chatham House Chatham House. The Royal Institute of International Affairs, July 2019.

[4] The Washington Treaty, April 4, 1949. Available at: https://www.nato.int/cps/en/natohq/official_texts_17120.htm

[5] NATO Brussels 2021 Summit Communiqué, June 14, 2021, para. 33. Available at: https://www.nato.int/cps/en/natohq/news_185000.htm

[6] NATO Strategic Concepts, updated on June 15, 2021, Available at: https://www.nato.int/cps/en/natohq/topics_56626.htm#:~:text=The%20current%20Strategic%20Concept,-The%202010%20Strategic&text=After%20having%20described%20NATO%20as,crisis%20management%20and%20cooperative%20security

[7] Strengthened Resilience Commitment, June 14, 2021. Available at: https://www.nato.int/cps/en/natohq/official_texts_185340.htm

[8] Y. Dinstein, A.W. Dahl, Section II: Cyber Operations. In: Oslo Manual on Select Topics of the Law of Armed Conflict. Springer, Cham, 2020. Available at: https://doi.org/10.1007/978-3-030-39169-0_2

[9] Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, opened for signature Jan. 27, 1967, 18 U.S.T. 2410, 610 U.N.T.S. 205 [hereinafter: Outer Space Treaty or OST]

[10] The Webster's New Collegiate Dictionary, Eleventh Edition, 2014.

[11] M. Schmitt, Sqn. Ldr. K. Tinkler, War in Space: How International Humanitarian Law Might Apply, The Woomera Project - Part 3, in Just Security, March 9, 2020, Available at: https://www.justsecurity.org/68906/war-in-space-how-international-humanitarian-law-might-apply/

[12] A. Stickings, Space as an Operational Domain: What Next for NATO?, October 2020, RUSI News brief, Vol. 40, No. 91. Available at: https://static.rusi.org/stickings_web_0.pdf

[13] NATO Recognized Cyberspace as a 'Domain of Operations' at Warsaw Summit, held on 8 – 9 July 2016. Available at: https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

[14] Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales, para.72; issued on September 5, 2014, updated in August 2018. Available at: https://www.nato.int/cps/en/natohq/official_texts_112964.htm

[15] London Declaration, December 4, 2019. Available at:

https://www.nato.int/cps/en/natohq/official_texts_171584.htm

[16] NATO's Approach to Space, NATO Official Website, 22 Apr. 2021. Available at: https://www.nato.int/cps/en/natohq/topics_175419.htm#:~:text=Space%20underpins%20NATO's%20ability%20to,companies%20based%20on%20their%20territory

[17] Foreign Ministers take decisions to adapt NATO, recognize space as an operational domain, 20 November 2019. Available at: https://www.nato.int/cps/en/natohq/news_171028.htm; Stoltenberg stated "What NATO will do will be defensive, and we will not deploy weapons in space", Martin Banks, NATO names space as an 'operational domain,' but without plans to weaponize it, November 20, 2019, in Defence News. Available at: https://www.defensenews.com/smr/nato-2020-defined/2019/11/20/nato-names-space-as-an-operational-domain-but-without-plans-to-weaponize-it/

[18] SHAPE, NATO Space Centre, Communiqué, October 2020. Available at: https://shape.nato.int/about/aco-capabilities2/nato-space-centre#:~:text=NATO%20Defence%20Ministers%20subsequently%20agreed,a%20meeting%20in%20October%202020.&text=NATO's%20new%20Space%20Centre%20is,to%20ensure%20its%20competitive%20advantage

[19] Dr. J. Donnelly, Lieutenant Commander J. Farley, Defining the 'Domain' in Multi-Domain, in Shaping NATO for Multi-Domain Operations of the Future, Joint Air & Space Power Conference 2019, on 8-10 October 2019, p.7. Available at: https://www.japcc.org/wp-content/uploads/JAPCC_Read_Ahead_2019.pdf. 'The NATO Combined Operations Planning Directive (COPD) uses the term domain in reference to the PMESII, which the JP 5-0 refers to as systems.

[20] Dr. S. Clarke, 'It's going to happen': is the world ready for war in space?, The Guardian, 15 April 2018. Available at: https://www.theguardian.com/science/2018/apr/15/its-going-to-happen-is-world-ready-for-war-in-space

[21] Schriever Wargame 2012, International HQ SACT Report. Available at: https://www.act.nato.int/images/stories/events/2012/sw12i/sw12i_report.pdf

[22] Cyber defence, NATO Official Website, 12 April 2021. Available at: https://www.nato.int/cps/en/natohq/topics_78170.htm

[23] Laura Brent, NATO's Role in Cyberspace, in NATO Review, February 12, 2019. Available at: https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.htm

[24] Joint Air & Space Power Conference 2021 Delivering NATO Air & Space Power at the Speed of Relevance,7-9 September 2021. Available at: https://www.japcc.org/cyberspace-and-joint-air-and-space-power

[25] Emerging and disruptive technologies, October 22, 2021. Available at: https://www.nato.int/cps/en/natohq/topics_184303.htm

[26] NATO Defence Ministers approve new space policy, discuss readiness and mission in Afghanistan, June 27, 2019. Available at: https://www.nato.int/cps/en/natohq/news_167181.htm

[27] Press conference by NATO Secretary General Jens Stoltenberg ahead of the meetings of NATO Ministers of Foreign Affairs, 19 Nov. 2019 (Available at: https://www.nato.int/cps/en/natohq/opinions_170972.htm?selectedLocale=ru

[28] Jens Stoltenberg, 'NATO will defend itself' (2019), Available at: https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en

[29] Á. M. Blanco, Col Dr D. Gallton, D. Reding, The Impact of Law on NATO's Space Power at the Speed of Relevance (Conference Read Ahead), Joint Air & Space Power Conference 2021 Delivering NATO Air & Space Power at the Speed of Relevance,7-9 September 2021. Available at: https://www.japcc.org/the-impact-of-law-on-natos-space-power-at-the-speed-of-relevance/

[30] B. E. Bowen, War in Space Strategy, Spacepower, Geopolitics, Edinburgh University Press, 2020.

[31] How is the Term "Armed Conflict" Defined in International Humanitarian Law?", in International Committee of the Red Cross (ICRC) Opinion Paper, March 2008. Available at: https://www.icrc.org/en/doc/assets/files/other/opinion-paper-armed-conflict.pdf

[32] Article 51, UN Charter, 1945. Available at: https://www.un.org/en/about-us/un-charter/full-text#:~:text=Article%2051,maintain%20international%20peace%20and%20security

[33] NATO Ministerial Meeting Brussels, 17 December 1992. Available at: https://www.bits.de/NRANEU/UN-NATO%20Peacekeeping/Brussels.htm

[34] Guiding Principles Art.4, in NATO Policy for the Protection of Civilians, endorsed by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016; Last updated: 24 Jun. 2021. Available at:

https://www.nato.int/cps/en/natohq/official_texts_133945.htm

[35] Guiding Principles Art. 11, in NATO Policy for the Protection of Civilians, endorsed by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8-9 July 2016; Last updated: 24 Jun. 2021. Available at: https://www.nato.int/cps/en/natohq/official_texts_133945.htm

[36] N. Tsagourias, R. Buchan, Research Handbook on International Law and Cyberspace, Edward Elgar Publishing, 2015.

[37] NATO Standardization Agreement (STANAG) 2449, on Training in the Law of Armed Conflict, June 26, 2019.

[38] Case Concerning Oil Platforms (Islamic Republic of Iran v. United States of America), the ICJ does not rule out the approach consisting in assessing whether a series of attacks against the United States can be categorised as an armed attack (Judgment, ICJ Reports, 2003, § 64). SGDSN, in Strategic Review of Cyberdefence, 2018, p. 82.

[39] Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities, Stimson Centre, July 29, 2013. Available at: https://www.stimson.org/2013/gge-report-transparency-and-confidence-building-measures-outer-space-activities/

[40] UN A/70/174, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, 22 July 2015. Available at: https://www.un.org/ga/search/view_doc.asp?symbol=A/70/174)

[41] International Law in the Cyber Domain, Parliamentary Documents, September 26, 2019. Available at: https://www.government.nl/binaries/government/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace/International+Law+in+the+Cyberdomain+-+Netherlands.pdf

[42] M. N. Schmitt, The Netherlands Releases a Tour de Force on International Law in Cyberspace: Analysis, in Just Security, October 14, 2019. Available at: https://www.justsecurity.org/66562/the-netherlands-releases-a-tour-de-force-on-international-law-in-cyberspace-analysis/

[43] D. Efrony, Y. Shany, 'A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice', (2018) 112 AJIL, pp. 583, 638.

[44] No 202 in Article 48 of ITU Constitution.

[45] No 203 in Article 48 of ITU Constitution.

[46] M. Manulis, C. P. Bridges, R. Harrison, V. Sekar, A. Davis, Cyber Security in New Space Analysis of Threats, Key Enabling Technologies and Challenges, in International Journal of Information Security, 12 May 2020. Available at: https://doi.org/10.1007/s10207-020-00503-w

[47] B. Unal, Cybersecurity of NATO's Space-based Strategic Assets, Research Paper, International Security Department, Chatham House, July 2019.

[48] V. R. Díez, Spoofing and jamming over GNSS, in INCIBE, 07.09.2020. Available at: https://www.incibe-cert.es/en/blog/spoofing-and-jamming-over-gnss

[49] Trident Juncture 18, NATO Official Website, 25 Oct. 2018 - 07 Nov. 2018. Available at: https://www.nato.int/cps/en/natohq/news_158620.htm; NATO launches biggest war games since end of Cold War. Available at: https://www.dw.com/en/nato-launches-biggest-war-games-since-end-of-cold-war/a-46033631

[50] B. Tinger, Electronic jamming between Russia and NATO is par for the course in the future, but it has its risky limits, in Atlantic Council, November 15, 2018. Available at: https://www.atlanticcouncil.org/blogs/new-atlanticist/electronic-jamming-between-russia-and-nato-is-par-for-the-course-in-the-future-but-it-has-its-risky-limits/

[51] S. F. Bichler, Mitigating Cyber Security Risk In Satellite Ground Systems, Paper Submitted for Master Of Operational Arts And Sciences, Advisor: Lt Col D. H. Maxwell Air Force Base, Alabama, April 2015.

[52] P. K. Martin, NASA Cybersecurity: An Examination of the Agency's Information Security, Testimony before the Subcommittee on Investigations and Oversight, House Committee on Science, Space, and Technology U.S. House of Representatives, February 29, 2012.

[53] Office of the Under Secretary of Defence, Cybersecurity Maturity Model Certification, march 2020. Available at: https://www.acq.osd.mil/cmmc/docs/CMMC_ModelMain_V1.02_20200318.pdf

[54] (AJP)-01 Edition E, Version 1, Allied Joint Doctrine, 2017, NATO Standardisation Office.

[55] R. Emmott, Exclusive: NATO aims to make space new frontier in defense, Reuters, AEROSPACE AND DEFENSE, June 21, 2019. Available at: https://www.reuters.com/article/us-nato-space-exclusive/exclusive-nato-aims-to-make-space-new-frontier-in-defense-idUSKCN1TM1AD