Research Paper

Beyza Unal
International Security Department | July 2019

Cybersecurity of NATO's Space-based Strategic Assets

CHATHAM HOUSE
The Royal Institute of International Affairs

Contents

Summary

- All satellites depend on cyber technology including software, hardware and other digital components. Any threat to a satellite’s control system or available bandwidth poses a direct challenge to national critical assets.

- 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. 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.

- Almost all modern military engagements rely on space-based assets. During the US-led invasion of Iraq in 2003, 68 per cent of US munitions were guided utilizing space-based means (including laser-, infrared- and satellite-guided munitions); up sharply from 10 per cent in 1990–91, during the first Gulf war. In 2001, 60 per cent of the weapons used by the US in Afghanistan were precision-guided munitions, many of which had the capability to use information provided by space-based assets to correct their own positioning to hit a target.

- NATO does not own satellites. It owns and operates a few terrestrial elements, such as satellite communications anchor stations and terminals. It requests access to products and services – 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.

- 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. 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.

1. Introduction

Space is a vital part of national and international infrastructures. Since the launch of the first artificial satellite, Sputnik 1, in 1957, humanity has used space for the purposes of communication, monitoring the environment, collecting intelligence, conducting vital scientific experiments, and providing data for global positioning, navigation and time keeping. Countries are increasingly dependent on global satellite capabilities for national and international infrastructures, which include systems governing the navigation of aircraft and ships, military manoeuvres, financial transactions, the internet and telecommunications.

Strategic space capabilities are generally composed of three elements: a space segment, a ground segment, and a user segment – also known as an uplink, a downlink and a crosslink – that transmit telemetry data.[1] Military commanders, staff and senior decision-making cadres within NATO receive mission-significant data through products[2] – e.g. space imagery and weather maps – and services[3] – e.g. satellite communications and position, navigation and timing (PNT) data – provided by member states with space capabilities. Although emerging technologies such as artificial intelligence (AI) and the Internet of Things (IoT) could be force multipliers for space capabilities,[4] increased prevalence of cyber means may also challenge the integrity of data carried through these technologies.

Most countries either own satellites or have a stake in space-based assets for meteorological purposes and communications.[5] The functioning of all satellites is dependent on cyber technology, including software, hardware and other digital components. Any threats that could impact a satellite's controls, reliability, or bandwidth availability would pose a direct challenge to national critical assets.[6] If cyberthreats are not effectively addressed, vulnerabilities in the strategic infrastructure could result in severe consequences for international security. Cyber vulnerabilities strike at the heart of the key technologies in strategic doctrines and military planning. In the event of crisis escalation, such as in Ukraine, the Middle East or in South Asia, the assumption is that weapons systems will perform as planned. But this should not be taken for granted. It is mission-critical for NATO to manage, preserve and protect space capabilities, *inter alia,* by means of agreements and policies. Understanding space vulnerabilities and ensuring that mitigation measures and redundancies are in place, will help to protect NATO's space capabilities.

NATO's missions and operations are conducted in four areas: air, land, cyber and sea.[7] Space-based architecture is fundamental to the provision of data and services to all domains. Therefore, any vulnerability in space infrastructure will likely spread to other domains.[8] The critical interdependency between space and other domains increases the threat of cyber risks, which disproportionately affect mission assurance. Investing in mitigation measures and in the resilience of space systems are key priorities in protecting all domains.

[1] NATO (2013), *NATO Space Handbook*, NATO Unclassified.

[2] Space products are the outputs, such as reports and imagery, of analysed and processed data by space-based sensors.

[3] Space services are the data that is provided from space assets to an end-user terminal.

[4] Force multipliers are the tools and assets that help an organization to amplify their efforts in order to achieve better outcomes.

[5] This paper uses the terms 'space-based systems' and 'space-dependent systems' interchangeably. Any system that uses space in its operations is viewed as a space-based system, irrespective of its geography (i.e. whether it is a space- or ground-based system).

[6] NATO (2014), *Space Support in NATO Operations: NATO Dependencies on Space*, NATO Unclassified.

[7] See, for instance, NATO (2018), *Joint Air Power Strategy*, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180626_20180626-joint-air-power-strategy.pdf (accessed 10 May 2019).

[8] Similarly, the cyber domain also cuts across land, air, and maritime domains within NATO's operations.

Since NATO relies on the space-based assets of its member states and allies, any consideration of mitigation measures – such as systems redundancy and increased technical resilience – would require the consent and involvement of all parties.

There is an urgent need to study and address cyber-related challenges to strategic assets within NATO and its key member countries, particularly the cyberthreat to space-based command and control systems. It is difficult to define what constitutes a country's strategic military assets. Depending on where they are deployed, even short- to medium-range ballistic missiles or tactical nuclear weapons may be viewed as strategic assets.

> There is an urgent need to study and address cyber-related challenges to strategic assets within NATO and its key member countries.

Strategic military systems depend heavily on space-based assets for navigation and targeting, timing, positioning, command and control, operational monitoring, intelligence gathering and reconnaissance, among other functions. However, the increasing vulnerability of space-based assets, ground stations, associated command and control systems, and the personnel who manage the systems, has not yet received the attention it deserves. This is particularly true in regard to the so-called 'New Space' revolution: the growing role of the private sector in space. For example, during the Iraq war of 2003–11, there was a 560 per cent increase in the US reliance on commercial satellites for military purposes.[9]

Policy influencers and policymakers are struggling to grasp the full impact of cyber vulnerabilities in the context of both space-based assets and strategic systems. Just as with physical attacks on space-based assets – such as anti-satellite weapon (ASAT) strikes[10] – cyberattacks have the potential to wreak havoc on strategic weapons systems and undermine deterrence by creating uncertainty and confusion. Cyberthreats pose a significant and complex challenge due to the absence of a warning and speed of an attack, the difficulty of attribution, and the complexities associated with carrying out a proportionate response. Given the progress made in the areas of strategic conventional weapon systems – for example, the development of advanced cruise missiles and hypersonic glide vehicles – it is essential for NATO and its allies to be able to rely upon space-based systems for early observation and detection; this may enable them to identify and attribute activities and to launch effective, calibrated responses. Cyber technology and innovation are accessible across much of the world, levelling the field and creating opportunities for states outside the NATO alliance – such as China, Russia and North Korea, for example – to instigate high-impact attacks on allied-owned strategic assets.

This research paper will first introduce the cyber risks to strategic systems, through an evaluation of threats, vulnerabilities and consequences. The paper aims to frame the problem by analysing ongoing incidents, and to conduct an analysis of threats and resilience measures in order to offset the risks. Second, it will discuss cyber risks for specific space-dependent strategic weapons systems. Third, it will explore mitigation measures against such cyber risks, through examining NATO's capability development approach, which is known as DOTMLPF-I (doctrine, organization, training, materiel, leadership, personnel, facilities, and interoperability).

[9] Johnson-Freese, J. (2007), *Space as a Strategic Asset*, New York: Columbia University Press, p. 29.

[10] Anti-satellite weapons (ASAT) aim to decapitate or destroy satellites by using kinetic means (such as missile defence interceptors) or by frequency jamming. In 2018, a research project conducted by the UN Institute for Disarmament Research (UNIDIR) proposed guidelines for the testing of ASAT technologies in order to sustain security in outer space. See Porras, D. (2018), *Towards ASAT Test Guidelines*, The Space Dossier, http://www.unidir.org/programmes/security-and-technology/the-space-dossier (accessed 10 May 2019).

2. Cyber Risks to Space-based Strategic Systems

Risk is a product of probability and consequence. However, since estimating the probability of a cyberattack is unreliable at best,[11] this paper focuses on the qualitative nature of potential threats, vulnerabilities and their impacts. Without knowing the actual likelihood of an event happening, it is still possible to assess threats and likely degree of exposure, which can identify potential resilience measures. In essence, the priority of NATO and its allies should be the readiness of their forces to identify potential threats and defend critical assets, rather than the likelihood of cyberattacks on space-based strategic systems. This approach minimizes risk by taking preparedness, resilience and continuity into the equation. Furthermore, it does not require detailed knowledge of an adversary’s motivation and capability.

Cyberattacks are a different beast to traditional forms of aggression. Whereas electronic attacks use physical means (such as jamming or ‘spoofing’) to interfere with the transmissions of radio frequency signals and cause reversible damage, cyberattacks employ digital manoeuvres to target data and access systems in order to cause permanent damage.[12] Electronic warfare methods can physically cut out communication signals that go to satellites (upstream) and come back from satellites (downstream). The attacker could send fake signals (spoofing) and trick the system without the knowledge of the receiver. In a cyberattack, however, an adversary would be able to gain full access to satellites as well as data, enabling them to cause permanent damage.[13]

Spoofing information through cyber means is a more sophisticated form of jamming. In times of conflict, global positioning system (GPS) digital spoofing – which involves digital interception and manipulation – permits the transmission of false information without the awareness of either the transmitter or the receiver. This approach could be used to disorient troops or even control their deployment. In order to mitigate risks, military forces should have the means to validate information integrity and detect spoofing and manipulation of data. One possible approach would be to educate and train personnel in alternative navigation methods as a minimum requirement for those working for NATO and its allies.

Cyberthreats to strategic systems

Cyber research is a fast-moving and constantly evolving area of science, and the scope of cyberthreats that countries face is on the rise as malicious actors find new ways to infiltrate weapons systems.

The use of electronic warfare methods and cyberattacks in peacetime illustrates the blurred lines of engagement between nations even in the absence of conflict. According to Norwegian military and NATO officials, Russia persistently jammed civilian GPS signals during NATO’s 2018 Trident Juncture exercise in Europe’s High North region, which highlights the growing threat. In November

[11] For more information on flaws of probability assessment, please read any article by Nassem Nicholas Taleb.

[12] For a detailed explanation, please see Harrison, T., Johnson, K., and Roberts, T. G. (2018), *Space Threat Assessment 2018*, Center for Strategic & International Studies, https://www.csis.org/analysis/space-threat-assessment-2018 (accessed 27 Mar. 2019).

[13] Ibid.

2018, NATO Secretary-General Jens Stoltenberg stated that electronic warfare and cyberattacks were increasingly being used in operations.[14] It was also reported that NATO officials believed Russia is testing this capability through its large-scale exercises, such as Zapad 2017, which was conducted jointly with Belarus in September 2017.[15]

According to the Consultative Committee for Space Data Systems (CCSDS), the most common cyberthreats to the space segment, ground segment and space-link communication segment include data corruption/modification; ground system loss; interception of data; jamming; denial of service; masquerade (spoofing); replay; software threats; and unauthorized access.[16] There is also crossover between offensive and defensive activities in cyberspace and space, given that – technologically – offence is easier and more cost-effective than defence.[17] Furthermore, space-related personnel are vulnerable to cyberthreats. Social engineering is becoming an important tool when used by adversaries, and – whether it occurs deliberately or unwittingly – the potential for people to constitute the weakest link in cyber defence is an increasing reality.[18]

The nature of cyber activities must evolve from being purely defensive to include active, persistent engagement, in order to disrupt attackers of western critical space-based capabilities. Given the importance of space-based systems to critical infrastructure that supports NATO military capabilities, it would be prudent to assume that an adversary is already active in these networks and focus on resilience measures. This increases urgency for advanced techniques, such as AI and machine learning (ML),[19] to identify and respond to modern threats.

Both China and Russia prioritize electronic warfare, cyberattacks and superiority within the electromagnetic battlespace as part of a strategy to achieve victory in future operations. Available doctrine from these nations highlights a key focus on preventing adversarial satellite-based communication systems from impacting their operational effectiveness[20] – a focus shared in US military planning and policy.[21]

Russian space capabilities and their cybertechnologies pose particular threats to NATO. For its navigational system, Russia relies on its own satellite system GLONASS (Global Navigation Satellite System), rather than the US-provided GPS or the EU's Galileo system. As part of a series of improvements to its communications technology and GLONASS, Russia is designing new navigation satellites, which are claimed to be highly accurate and longer lasting.[22] Russia has

[14] Tigner, B. (2018), 'Electronic Jamming Between Russia and NATO is Par for the Course in the Future, But it Has its Risky Limits', Atlantic Council, 15 November 2018, http://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 (accessed 19 Nov. 2018).

[15] Ibid.

[16] The Consultative Committee for Space Data Systems (CCSDS) (2015), *Report Concerning Space Data System Standards – Security Threats against Space Missions*, https://public.ccsds.org/Pubs/350x1g2.pdf (accessed 23 May 2019); Livingstone and Lewis (2016), *Space, the Final Frontier for Cybersecurity?*

[17] Baylon, C. (2014), *Challenges at the Intersection of Cyber Security and Space Security: Country and International Institution Perspectives*, Research Paper, London: Royal Institute of International Affairs, https://www.chathamhouse.org/sites/files/chathamhouse/field/field_document/20141229CyberSecuritySpaceSecurityBaylonFinal.pdf (accessed 19 Nov. 2018).

[18] It is important to acknowledge that when organizations incorporate into their cyber strategies the significance of personnel in mitigating cyber risks, those personnel may become the strongest link in defending against cyberattacks.

[19] Machine learning is a subset of AI. Machine learning approaches in the military domain are currently challenging as they require a large set of information and military applications are either short of data or do not share data with third parties. For more information on artificial intelligence and machine learning, see Boulanin, V. (ed.) (2019), *The Impact of Artificial Intelligence on Strategic Stability and Nuclear Risk*, SIPRI, pp. 13–22, https://www.sipri.org/publications/2019/other-publications/impact-artificial-intelligence-strategic-stability-and-nuclear-risk (accessed 31 May 2019).

[20] Office of the Secretary of Defense (2018), *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2018*, US Department of Defense, https://media.defense.gov/2018/Aug/16/2001955282/-1/-1/1/2018-CHINA-MILITARY-POWER-REPORT.PDF (accessed 10 May 2019).

[21] Curtis E. LeMay Center for Doctrine Development and Education (2012), *Annex 3-14 Space Operations*, United States Air Force, https://fas.org/irp/doddir/usaf/3-14-annex.pdf (accessed 30 Apr. 2019).

[22] Harrison, Johnson and Roberts (2018), *Space Threat Assessment 2018*; Kurskov, E (2019), 'New generation satellites to join GLONASS system early 2020', TASS, 9 April 2019, http://tass.com/science/1052778 (accessed 30 Apr. 2019).

been testing its capabilities in a hybrid context in Syria and in Ukraine, particularly relying on capabilities for jamming GPS signals to ground remotely piloted aircraft. It is reported to have conducted denial-of-service attacks on radio and telephone equipment, and to have attempted to steal encrypted military data.[23]

> It is likely that several countries – such as the US, Russia and countries within the EU – will in future possess working quantum communications satellites.

China, too, is improving its space capabilities by investing in new areas of research, such as quantum communications satellite technology, which provides a new way to encrypt information transmitted between satellites, increasing the difficulty of hacking information.[24] In this regard, China's Micius satellite, the first of its kind when it was launched in 2016, may eventually be able to provide a quantum cryptography service.[25] Other countries are following suit and it is likely that several countries – such as the US, Russia and countries within the EU – will in future possess working quantum communications satellites. The European Space Agency, for instance, signed a contract with Luxembourg-based SES Techcom SA to develop a quantum cryptography telecommunication system (to be known as QUARTZ).[26] With this agreement, quantum communications have opened a new dimension in cryptography. Quantum capabilities are likely to make existing asymmetric-based, traditional cryptographic-based protection obsolete. The EU, the UK and the US are all investing heavily in a range of quantum technologies – including communication devices, computers and imaging enhancers.

Vulnerabilities to strategic systems

When analysing risk, understanding system vulnerabilities is as important as understanding the threat landscape. Threats alone would not pose a risk if there were no known vulnerabilities for an adversary to exploit. Similarly, system vulnerabilities would not always result in risk, especially in peacetime, when there is no incentive to attack or infiltrate.

In the military domain, some of the major system vulnerabilities include the use of commercial companies for military purposes; 'back-doors' in encryption; and the supply-chain security of satellites.[27] This list can also be extended to include physical, personnel and procedural vulnerabilities. Risks also arise from the dual-use aspect of most of the space-related technology – where the technology can be used for both civilian and military purposes. For instance – whether fixed or mobile units – communications satellites and broadcasting satellite services have both civilian and military utility. Similarly, the utilization of satellite imagery capability in the civilian sphere for earth observations, environmental monitoring, and the provision of oceanographic and cartographic data, also extends to the military domain.[28] There is an increasing need to apply higher-grade military hardening and cyber protection specifications to civilian capabilities that have the potential to be used in support of military applications.

[23] Leicester, J. (2018), "Espionage': French defense head charges Russia of dangerous games in space', *Defense News*, 7 September 2018, https://www.defensenews.com/space/2018/09/07/espionage-french-defense-head-charges-russia-of-dangerous-games-in-space/ (accessed 30 Apr. 2019).

[24] Wall, M. (2016), China Launches Pioneering 'Hack-Proof Quantum Communications Satellite', Space.com, 16 August 2016, https://www.space.com/33760-china-launches-quantum-communications–satellite.html (accessed 28 Dec. 2018).

[25] MIT Technology Review (2018), 'Chinese satellite uses quantum cryptography for secure videoconference between continents', https://www.technologyreview.com/s/610106/chinese-satellite-uses-quantum-cryptography-for-secure-video-conference-between-continents/ (accessed 28 Dec. 2018).

[26] European Space Agency (2018), 'Space Protons Bring a New Dimension to Cryptography', https://www.esa.int/Our_Activities/Telecommunications_Integrated_Applications/Space_photons_bring_a_new_dimension_to_cryptography (accessed 28 Mar. 2019).

[27] Livingstone and Lewis (2016), *Space, the Final Frontier for Cybersecurity?*

[28] Johnson-Freese (2007), *Space as a Strategic Asset*, p. 31.

These capabilities aside, terminals located in ground stations constitute a critical vulnerability, as a terminal is an access point to a satellite and is usually not protected by authentication in order not to hinder operational actions. Terminals house software systems that can be compromised and require patching and upgrading. Moreover, software embedded in weapons systems (such as precision-guided munitions) could also be compromised.

At times, NATO allies procure equipment and software to be integrated into their national defence architecture, which becomes part of the overall NATO capability. The commercial supply chain is embedded in nearly every aspect of military equipment. This may not necessarily be a particular vulnerability, as long as commercial equipment is designed to military standards and is secure. However, if military standards are not met, items procured from commercial industry with design flaws may expose NATO's systems to additional vulnerabilities.

> While the absence of data is easy to detect, the manipulation of data or erosion of confidentiality at such an interface is potentially more difficult to discern.

Civil satellites, operated by private companies, may be used to fulfil specific missions in locations where NATO allies do not have their own space equipment. Ground stations constitute further elements that are relevant for the data flow. From a cybersecurity point of view, each interface could present a vulnerability and could become a weakness, as an interface typically requires manual processes to establish its operation, and/or the administration of the components involved. Adversaries infiltrating ground- or space-based systems could exploit weak software implementation, or the incompatibility of network or data transfer protocols in the chain. While the absence of data is easy to detect, the manipulation of data or erosion of confidentiality at such an interface is potentially more difficult to discern. Vulnerabilities can stem from:

- A higher number of data exchange interfaces used between the military and civil sectors;
- The fact that each actor has its own isolated view of its data network, protected by its own security standard;
- The use of old and proprietary IT hardware and software; and
- The failure or inability to conduct regular software updates to remove known vulnerabilities.

In such an environment, it seems difficult to ensure security of the information delivered.

Space-specific risks for the NATO alliance and for key NATO countries

Space systems, which include both satellites and ground stations, as well as related space products and services, provide mission-critical information both for NATO's member states and for the alliance as a whole. NATO relies on space-based assets for almost all of its operations and missions.[29] Some of the critical missions that rely on space assets include: defence of NATO's territory and the neighbouring regions; peacekeeping missions; humanitarian assistance and disaster relief; counterterrorism; and conflict prevention activities.

[29] NATO (2014), *Space Support to NATO Operations: NATO Dependencies on Space*, NATO Unclassified.

NATO does not own satellites. It owns and operates a few terrestrial elements, such as satellite communications (SATCOM) anchor stations and terminals. It requests access to products and services but does not have direct access to satellites, leaving it up to its allies to determine whether they provide access to their satellite capabilities. NATO has established memoranda of understanding with allies for possible use of space products and services.

Originally, in the US, space systems used by the military were separated from commercial and civilian assets in terms of their development and operation.[30] One of the reasons for this separation was to protect the military structure against physical and cyberthreats. Military space system safety and security requirements were also higher and more stringent than in the commercial sphere (for example, requirements to invest in survivability enhancement mechanisms in order to resist jamming, or special design approaches for military space architecture). In recent years commercial methods, for instance the capture and analysis of satellite imagery, have been shown to be as effective as military means. As a result, NATO uses a mix of military, civilian, commercial, and national/multinational assets to conduct its operations. The joint use of these assets, however, comes with an acceptance of inherent risk, not only to the countries that provide such capability but also to the alliance as a whole. In response, the European Defence Agency, through its Governmental Satellite Communications (GOVSATCOM) development programme, decided to build an intermediary class of satellites between commercial SATCOM and military SATCOM, with security requirements able to address the needs of critical missions, including crisis management.[31]

There is increased dependence on space-based systems in modern military engagement. During the US engagement in Iraq in 2003, 68 per cent of munitions were guided utilizing space-based means (including laser-, infrared- and satellite-guided munitions); this percentage had risen sharply from 10 per cent in 1990–91, during the first Gulf war.[32] In its operations in Afghanistan in 2001, 60 per cent of the weapons used by the US were precision-guided munitions: these included bombs, missiles, and other weapons, many of which had the capability to correct their own positioning to hit the target, using space-derived information.[33]

> Cyber vulnerabilities undermine confidence in strategic systems; they increase uncertainty in information and analysis, which impacts the credibility of deterrence and strategic stability. Loss of trust in technology also has implications for attribution and strategic calculus in crisis decision-making and may increase the risk of misperception.

This dependency on space-based technology has major implications for the way NATO conducts warfare today, and how it will do so in the future. For instance, in order to conduct precision strikes or earth observation through the use of unmanned aerial vehicles (UAVs – such as military drones), systems rely on so-called 'beyond-line-of-sight' (BLOS) communication via satellites – especially

[30] James, Lt-Col. L. D. (1993), *DOD Space Systems – Reducing the Cost*, Air War College, Air University, Unclassified, www.dtic.mil/dtic/tr/fulltext/u2/a283159.pdf (accessed 10 May 2019).

[31] European Commission (2018), *Commission Staff Working Document: Impact Assessment: GOVSATCOM, establishing the space programme of the European Union, relating to the European Union Agency for Space and repealing Regulations (EU) No 1285/2013, No 377/2014 and No 912/2010 and Decision 541/2014/EU*, p. 4, https://publications.europa.eu/en/publication-detail/-/publication/6204a2f1-6af6-11e8-9483-01aa75ed71a1/language-en/format-PDF (accessed 30 May 2019).

[32] UK Parliamentary Office of Science and Technology (2006), 'Military Uses of Space', Postnote, Number 273, December 2006, http://www.parliament.uk/documents/post/postpn273.pdf (accessed 30 May 2019).

[33] Huiss, R. (2012), 'Proliferation of Precision Strike: Issues for Congress', Congressional Research Service, p. 6, https://fas.org/sgp/crs/nuke/R42539.pdf (accessed 10 May 2019).

in times of crisis and conflict, since ground-based line-of-sight communications are vulnerable to physical attacks. Yet, cyberattacks on space technology or on the UAVs may lead them to misinterpret commands, or to lose contact with the command centre and fail in operation.

NATO currently uses six space-dependent capabilities for its alliance operations and missions:

- Position, navigation and timing (PNT)
- Intelligence, surveillance and reconnaissance (ISR)
- Missile defence
- Communications
- Space situational awareness (SSA)
- Environmental monitoring (weather forecasting)

The core functioning of these six capabilities for NATO operations includes:

- Providing communication in military operations and missions, for instance between a commander and their troops;
- Providing early warning, through detecting the hot plumes of a ballistic missile launch – thus, increasing the time available to respond to an upcoming threat;
- Providing a precise location for targeted strikes;[34]
- Providing imagery of targets, in order to observe, detect and analyse their status (situational awareness);
- Providing GPS for weapon guidance;
- Providing timing for secure communications; and
- Providing space surveillance and tracking.

The table below outlines the key roles for each capability:

Table 1: NATO space-dependent capabilities and their roles

NATO space-dependent capabilities	Role
Position, navigation and timing (PNT)	• Provide information for a precision strike. • Support targeting information. • Synchronize operations. • Provide network timing and communication data. • Rely on GPS for accurate frequency, timing and synchronization. • Track assets and forces. • Provide maritime navigation data. • For instance, PNT is fundamental for combat search and rescue (CSAR) missions.

[34] NATO forces rely on GPS for this function.

NATO space-dependent capabilities	Role
Intelligence, surveillance and reconnaissance (ISR)	• Intelligence assessment and support threat intelligence. • Situational awareness in all four domains as well as space. • Targeting information. • Signal intelligence (SIGNIT) collection. • Intelligence for the electromagnetic environment. • Use of ISR visual, multi- and hyperspectral radar imagery for command, control and communication (C3) across core domains. • For instance, satellite imagery analysis has been used by military, civilian and commercial organizations to identify North Korea's nuclear weapons and missile-related activities.
Missile defence	• Assess ballistic missile (BM) attacks. • Support to early warning and assessment of BM attacks or attacks on space systems. • Support to early warning of nuclear detonations.
Communications	• Support of command and control (C2) for radio communications. • Support communications in all domains. • Used for unmanned vehicle operations.
Space situational awareness (SSA)	• Explore space debris, space surveillance and tracking. • Observe multiple data types and sources on space to achieve awareness. • Detect threats to space-borne assets, to astronauts and to Earth. • Observe space weather, as it may interrupt services, impact radio signals or damage satellite applications. • Outer space-based observation to detect threats from adversary space-based platforms. • Ensure integrity of systems in light of the increasing amount of 'space junk' or potential adversary space-based weapon systems.
Environmental monitoring (weather forecasting)	• Provide weather forecasting, geospatial and maritime information (both space and terrestrial weather). • Provide space weather information. • Support mission planning and targeting. • Support munitions selection. • For instance, maps developed in Afghanistan helped to predict future flooding: this information was used both for assisting military operations and for humanitarian assistance/disaster relief cases.[35]

Identification is another important capability that is used in the NATO maritime domain for coastal tracking, and for identifying and locating ships and vessels. Using automatic identification systems (AIS), data is electronically transmitted between ships and the coastal stations. By providing similar functions, AIS supplements and provides resilience to maritime radar and is fundamental for avoiding collisions.[36]

NATO's space-dependent capabilities have individual functions, as described above. These capabilities are also coupled to each other, with complex cross-dependencies, so that the loss of one capability may have a collateral impact on other capabilities. For instance, most of the assets that transmit communications to support command and control are also dependent on GPS for timing and synchronization.[37] Although there would be a number of contenders for technologies of utmost importance to NATO missions and operations, preliminary research indicates that PNT signals (which utilize GPS) are a much-needed priority capability in almost all NATO operations.

[35] NATO (2014), *Space Support to NATO Operations: NATO Dependencies on Space*.
[36] Morris, B. (2016), 'AIS versus radar', Ocean Navigator, http://www.oceannavigator.com/Web-Exclusives-2016/AIS-versus-radar/ (accessed 10 May 2019).
[37] NATO (2014), *Space Support to NATO Operations: NATO Dependencies on Space*.

3. Analysis of Space-dependent Capabilities for NATO Missions and Operations

Position, navigation and timing (PNT)

PNT is a vital part of any NATO operation. It provides forces with the necessary means to conduct timely and effective operations. Thus, the loss of PNT would leave forces vulnerable to attacks.

NATO uses GPS for accurate timing and navigation in its PNT system. The accuracy of this data depends on the satellite geometry and the receiver system. In the tactical domain, alliance troops may not always have – or be able to rely on – space capabilities in conducting their missions. For instance, during a NATO exercise in Finland in 2018, Finland's civilian air navigation services were disrupted through electronic means, which was later attributed to Russia.[38] Loss of navigation capability was also reported in Norway at the same time. While these incidents were not cyberattacks, they illustrate the extent of NATO forces' dependency on navigational signals, and the vulnerability of navigation systems to interference.

> At the very beginning of its development, the US claimed that Galileo would be superfluous to the already existing GPS capability and that it would rival the capabilities of the US by creating a reduced European security reliance on that country.

In 2002, the EU initiated a European alternative to GPS, named Galileo,[39] which is one of four existing Global Navigation Satellite Systems (GNSS). At the core of Galileo lies a European strategic determination to create a stand-alone system that is independent from but compatible with the US's GPS system, thus providing much-needed resilience for both the US and Europe. At the very beginning of its development, the US claimed that Galileo would be superfluous to the already existing GPS capability and that it would rival the capabilities of the US by creating a reduced European security reliance on that country. Later, this policy was dropped as it became increasingly obvious that Galileo provided a necessary back-up system for GPS – a parallel route for space resilience, and therefore for trans-Atlantic security. There is a need for GPS/Galileo interoperability for NATO military capabilities that are dependent on space-based systems to ensure their reliability and integrity. Galileo has a civilian portion and a public regulated service (PRS), which is an encrypted navigation service, restricted to governments

[38] Woody, C. (2018), 'Finland and Norway are telling airline pilots to be ready to fly without GPS, and some think Russia is up to something', Business Insider, https://www.businessinsider.com/finland-norway-tell-pilots-to-fly-without-gps-and-some-blame-russia-2018-11?r=US&IR=T (accessed 17 Jun. 2019).

[39] The UK's decision to leave the EU creates a hurdle for Britain and the EU, as Britain was one of the biggest contributors of the Galileo programme. It is reported that the UK has invested around £1.2 billion into the Galileo system, which corresponds to one-ninth of the overall cost. During negotiations with the EU, Britain expressed its wish to continue to have access to the secure public regulated service (PRS) and to be involved in the development of Galileo even after leaving the EU. Michel Barnier, the EU chief Brexit negotiator, indicated that the EU would be open to negotiation with the UK on access to the PRS service, similar to the negotiations with the US and Norway over their access to Galileo. There is no obstacle for the UK to be a passive user of the Galileo system. In other words, the UK can still pursue the PRS access for defence and critical national infrastructure. The problem seems to be the UK's ambition to be involved in the future developments of Galileo so that the British military would not be vulnerable to foreign design technology.

that use it mainly in military applications.[40] PRS has anti-jamming and anti-spoofing capabilities, and is reserved for certain users within EU member states. The US needs to negotiate access to the PRS signals. When and if GPS fails to operate, Galileo is designed to provide civilian and military services for the US as well as for Europe. There is no interoperability issue between Galileo and GPS, as these points were discussed and solved in the framework of the EU–US agreement of 2004. The US needs to negotiate access to PRS signals. There is no agreement yet for Galileo to replace GPS in case of the latter's failure.

Intelligence, surveillance and reconnaissance (ISR)[41]

ISR provides information and imagery intelligence to allied forces about specific targets. It is used in air, land and maritime domains in order to supply accurate and timely information to the relevant commander to support decision-making.[42] NATO's intelligence-led operations rely fundamentally upon space-based ISR capabilities, and the effectiveness of the alliance's operations is based upon the availability of these systems.

The imagery that ISR provides can be used both in conventional and nuclear weaponry command and control, and in targeting. ISR capability is composed of airborne imagery platforms, space-based assets and ground sensors. The information is collected through surveillance and reconnaissance sensors, which may be vulnerable to cyberattacks. Sensors could also be manipulated through physical or cyber means: this could even occur at the design stage within the manufacturing organization – a weakness all NATO countries should be aware of, especially if they rely on equipment sourced from non-NATO parties for the components of intelligence-gathering technologies.

NATO is working to improve the interoperability of ISR capabilities. To this end, in 2011, nine NATO countries voluntarily joined the Multi-intelligence All-source Joint Intelligence Surveillance and Reconnaissance Coalition (MAJIIC-2) initiative, with the aim of increasing interoperability and information-sharing between each nation's ISR capabilities.[43] ISR technologies contribute significantly to national, regional and international security. Through surveillance systems, such technologies can observe and map adversary command, control and communication systems, thus providing invaluable strategic insights. Yet – as stated by a former battalion intelligence officer – collecting all the necessary information from multiple sources in a timely manner is not an easy task.[44] That information may be received at different times from different outlets. Technology is an important factor in facilitating this analysis, and AI can overcome many existent analytical difficulties and analyse data in a compressed time frame. Any loss of ISR capability through cyberattacks would have dire consequences for strategic planning and policy.

[40] European Global Navigation Satellite Systems Agency (n.d.), 'What is GNSS? PRS', https://www.gsa.europa.eu/security/prs (accessed 27 Mar. 2019).

[41] The US Department of Defense (DOD) defines ISR as 'an [...] activity that synchronizes and integrates the planning and operation of sensors, assets and processing, exploitation, and dissemination systems in direct support of current and future operations.' See Office of the Chairman of the Joint Chiefs of Staff (2019), DOD Dictionary of Military and Associated Terms, Washington, DC: The Joint Staff, April 2019, p. 113, https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf (accessed 30 May 2019).

[42] Mitchell (2011), *Persistent Intelligence, Surveillance and Reconnaissance (P-ISR)* p. viii.

[43] These nine nations comprise of Canada, France, Germany, Italy, the Netherlands, Norway, Spain, the UK and the US. See NATO Communications and Information Agency (2015), 'MAJIIC 2: Enhancing technical interoperability', NCI Agency video via YouTube, https://www.youtube.com/watch?v=-SnMTl0ajk4 (accessed 10 May 2019).

[44] Mitchell, J. (2011), *Persistent Intelligence, Surveillance and Reconnaissance (P-ISR): Debunking the Myth, Establishing the Concept, and Achieving the Possible*, p. viii.

Missile defence

Missile defence relies heavily on early warning capabilities otherwise known as integrated threat warning and threat assessment (ITW/TA): US space-based infrared sensors detect the hot plumes of ballistic missile launches and communicate the information to the service component command.

Theatre missile defence, which includes the Patriot missile defence system – a long-range surface-to-air missile system used by the US and NATO allies – and standard missile defence systems, and which is part of the naval component of the integrated Aegis weapon system, also serves as part of overall missile defence capability.[45] The Aegis combat system operates in the maritime domain, using radar to track and guide weapons to destroy targets; its elements – which include a space tracking and surveillance system, the AN/SPY-1A radar, a command and decision system and a display system – could all potentially be exposed to cyberattacks.

The US Department of Defense conducted an auditing exercise in 2018 for the internal controls of its ballistic missile defence systems (BMDS). The aim of the audit was to ensure that systems and programmes were functioning as intended. The findings indicated that there were 'internal control weaknesses related to protecting networks and systems that process, store, and transmit BMDS technical information'.[46] These weaknesses could be exploited through insider threat and/or cyber means.

Missile defence systems may fail, or they may be activated due to false information sent from communication systems (such as ground-based radars) to the command unit. The Israeli anti-missile defence system Iron Dome, for example, is claimed to have a 90 per cent accuracy rate when intercepting targets. Yet there have been cases where a faulty response within the system has activated the launch of interceptor missiles erroneously, such as occurred in Gaza in March 2018, when it was triggered by machine gun fire.[47] Thus the battle management and weapons control system was proved at that time to be unable to make proper threat assessments. Similar outcomes could result if the threat assessment control system is interfered with via cyber means; the consequences could be much higher, including the loss of civilian life. In the Israeli case, it was reported that Rafael Advanced Defense Systems, a supplier of technology to the Iron Dome system, together with Israel Aerospace Industries and the Elisra Group, both of which were also involved in the project, faced persistent cyberattacks during the period of October 2011 to August 2012. This resulted in the loss of sensitive data that was believed to include the specifications of the Arrow 3 missile, developed jointly by the US and Israel.[48] Vulnerability to cyberattacks within the supply chain is not unique to NATO, and NATO and its allies should address this type of risk. Supply chain integrity (in terms of both hardware and software) is imperative for reliable military systems.

One of the core elements of a missile defence system is that it relies on the reception of near real-time information by a command centre to be able to identify and project the trajectory of an incoming missile. Through automated response it calculates the speed, velocity and location of the target in order to be able to intercept the incoming missile in a short time frame. Any deliberate interference with the information,

[45] US Department of Defense (n.d.), 'Elements: Aegis Ballistic Missile Defense', Missile Defence Agency, https://www.mda.mil/system/aegis_bmd.html (accessed 28 Mar. 2019).

[46] US Department of Defense (2018), 'Security Controls at DoD Facilities for Protecting Ballistic Missile Defense System Technical Information', https://media.defense.gov/2018/Dec/14/2002072642/-1/-1/1/DODIG-2019-034.PDF (accessed 17 Apr. 2019).

[47] Ahronheim, A. (2018), 'IDF Says Iron Dome Launch in Response to Gunfire Not a Malfunction', *Jerusalem Post,* 26 March 2018, https://www.jpost.com/Arab-Israeli-Conflict/IDF-says-Iron-Dome-launch-in-response-to-gunfire-not-a-malfunction-547133 (accessed 28 Mar. 2019).

[48] Gibbs, S. (2014), 'Chinese hackers steal Israel's Iron Dome missile data', *Guardian*, 29 July 2014, https://www.theguardian.com/technology/2014/jul/29/chinese-hackers–steal-israel-iron-dome-missile-data (accessed 28 Mar. 2019). IAI refused this claim: please see Jerusalem Post Staff (2014), 'IAI Refutes Claim that Iron Dome Makers Were Hacked', Jerusalem Post, 31 July 2014, https://www.jpost.com/Defense/IAI-refutes-claim-that-Iron-Dome-makers-were-hacked-369505 (accessed 28 Mar. 2019).

for instance from the radar, could mean that the defence missiles fail to intercept an incoming threat, or could lead to a faulty decision based on falsified or spoofed information. Thus, for example, a defence missile could fail to hit the correct target and strike well beyond the intended target zone. In order to detect deliberate interference or cyber intrusion, it is important to put preventive measures in place. One such measure could be to conduct organized, simulated cyberattacks on a system to assess its performance: this is known as penetration testing. In the future, detection of anomalies could be possible through ML and AI, especially in closed networks.[49]

Communications

With the exception of anti-terrorism missions, all NATO missions rely on space-based communications. Within the NATO lexicon, an anti-terrorism mission is different to a counter-terrorism mission.[50] Whereas an anti-terrorism mission involves preventive and defensive measures to protect the NATO alliance's forces and reduce their vulnerability, a counterterrorism mission involves offensive measures that require space-based support.[51] Communications support strategic, operational and tactical decision-making, as well as the planning and direction of operations.

> With the exception of anti-terrorism missions, all NATO missions rely on space-based communications.

NATO owns and operates two Network Control Centres, which are responsible for satellite network planning, network control and ground segment management. Being able to rely on two facilities instead of just one increases resilience and the chance of system survivability (in the face of both physical attacks and cyberattacks).

NATO owns ground stations for SATCOM operations, but does not own satellites. It makes use of SATCOM assets, some of which are leased to NATO by the allies through memoranda of understanding, or by commercial service providers. For instance, the UK, French and Italian governments provide advanced SATCOM capabilities.[52] Thus, NATO has high levels of dependency on key allies and on their willingness to provide space-sourced data, information and services in general. In addition, space service agreements face several challenges, such as distribution restrictions, data licensing issues, and regulations on selling national resolution data.[53]

NATO's dependency on individual allies for the provision of such capacity creates problems, since different procedures may have to be followed in each case with regards to the types of data that can be shared with NATO. Thus, the dependency on communications assets rests more with the allies than with NATO. Yet, the vulnerability that may result from such dependency may equally affect NATO, all the allies and the individual member states that own satellites.

[49] Yet, it is possible to compromise the 'learning' process, especially in open networks. This may result in poor detection of anomalies. For more information on ML, see Mantere, M., Uusitalo, I., Sailio, M. and Noponen, S. (2012), 'Challenges of Machine Learning Based Monitoring for Industrial Control System Networks', 26th International Conference on Advanced Information Networking and Applications Workshops, doi: 10.1109/WAINA.2012.135 (accessed 10 May 2019).

[50] Please see NATO (2014), *Space Support to NATO Operations: NATO Dependencies on Space*.

[51] Ibid.

[52] NATO (2011), 'SATCOM Post-2000: Improved Satellite Communications for NATO', https://www.nato.int/cps/en/natohq/topics_50092.htm (accessed 10 May 2019).

[53] Essad, R., Kreitmair, T. and Patten L. (2013), 'Space Support to Operations-MAJEX13 Final Exercise Report', NCI Agency, Technical Report TR/2013/SPW009274/02, The Hague, Unclassified.

Space situational awareness (SSA)

Although space situational awareness (SSA) is not named as a core capability by NATO, its utility is acknowledged informally. Currently, NATO does not have a role in providing SSA; however, allies are developing their own capabilities.

SSA provides the necessary information about space assets, space weather conditions and debris that may pose threats to satellites. It is defined as 'the ability to view, understand and predict the physical location of natural and manmade objects in orbit around the Earth, with the objective of avoiding collisions.'[54] In other words, SSA provides information about natural and artificial objects in space, about the threats they pose and about the space environment in general.

SSA is used in both the civilian and military sectors. It has three specific purposes: providing space surveillance and tracking of space debris (objects) that circle around the Earth; providing space weather reports (see next section); and detecting near-Earth objects that risk causing damage on Earth. Through the observations made, the space-based infrastructure is prevented from colliding with space debris. Therefore, in order to avoid collisions with space debris or in order to move satellites, NATO and the allies require ongoing situational awareness in space. The US and the EU both conduct SSA activities so as to ensure safe and secure space activity.

Environmental monitoring

An area often neglected in discussions of space-dependent capabilities is the environmental monitoring of Earth: this process provides weather forecasting, geospatial and oceanographic information. Environmental monitoring is equally important during peacetime and during conflict. This capability supports mission planning, flight trajectories and targeting. For instance, in the context of NATO operations, environmental monitoring could supply information on flooding trends in a specific region, which a commander could access, allowing the latter to plan a mission accordingly. Weather information is also crucial to air defence planning and to the deployment of security against the use of chemical, biological, radiological and nuclear (CBRN) agents. Real-time weather data is vital for missile launches and accurate targeting. NATO does not itself supply data or equipment for the provision of weather-related information. Instead, information about environmental conditions – and their potential impact on SATCOM and sensor accuracy – is provided to NATO by the US, through the meteorological and oceanographic (METOC) community.[55]

Possible consequences of cyberattacks for NATO's space capabilities

Considering that digital technologies are fundamental to all six of the space-dependent capabilities described above, none of them is immune to cyberattacks. Moreover, any digital system that relies upon near real-time information is vulnerable to cyberattacks. The loss of one or more of these capabilities because of human or system error or through offensive cyber operations conducted by an adversary, could have severe strategic, operational and tactical consequences. In order to understand the value of each space-dependent capability, it is important to analyse the consequences of cyberattacks on each.

[54] Brancati, M. (2017), 'Space Situation Awareness & Space Surveillance Tracking, Telespazio & ThalesAlenia Space', presentation, http://www.cesmamil.org/wordpress/wp-content/uploads/2017/05/9-_-Matarazzo-Brancati-_-Thales-Telespazio.pdf (accessed 10 May 2019).

[55] US Joint Forces Command (2011), *Joint Meteorological & Oceanographic (METOC) Handbook*, 1st JMOC Edition, April 2011, https://www.jcs.mil/Portals/36/Documents/Doctrine/pams_hands/metoc_hbk.pdf (accessed 10 May 2019).

Cyberattacks on military weapons systems may have operational and strategic consequences that change the way the military operates in conflict. Although electronic warfare has been in use for more than a century,[56] sophisticated cyberattacks on the systems of NATO or its key member countries have a new and distinct impact on decision-making and on how NATO conducts its operations. Cyberattacks on military systems could also have a paralysing effect on strategic military and political decision-making and could render NATO countries vulnerable to Russian or Chinese information and deception operations.

Timing is a crucial element of PNT capability. Most of the electronics used in military, civilian and commercial spheres depend on timing signals. By intercepting securely transmitted data through cyber means, an adversary may jeopardize the alliance's missions and services. A compromised system would also diminish reliance on data received, as data confidentiality would be brought into question through possible acts of spoofing and deception.

The involvement of Russia and the US in the Syrian conflict, and the use of electronic techniques, such as signal jamming,[57] and cyber means, such as hacking and spoofing, demonstrates the potential operational uses of cyberattacks. Russia's electronic warfare capability involves not only an air defence capability but also integrates cyber operations.[58]

What type of consequences would result from cyberattacks within space-based systems? What would be the operational and strategic impact? The table below outlines some of the potential consequences for each capability:

Table 2: NATO space-dependent capabilities and potential consequences from their absence

NATO space-dependent capabilities	Potential impact from the loss of capabilities
Position, navigation and timing (PNT)	• Impacts on the civilian airspace, such as airliners losing on-board navigation systems (which is not directly within NATO's purview, but which would affect the scale of the conflict or crisis in general. Moreover, an attack on civil systems could result in military consequences). • Losing contact with the alliance's forces and assets during their deployment. • Loss of the time signal and its impact on the functioning of warships and guided missiles. • Losing connection with ships, aircraft, carriers etc. in conflict due to interference to their navigation systems. • Loss of precise time to create financial transaction timestamps as financial sector's internal clocks rely on GPS. • Cyberattacks on the guidance mechanism of a weapon (such as a missile) that would result in failure of weapons delivery accuracy. • Impact on the security of mission-critical assets and mission assurance.[59]

[56] Evans, G. (2018), 'The evolution of electronic warfare: a timeline', Army Technology, 7 June 2018, https://www.army-technology.com/features/evolution-electronic-warfare-timeline/ (accessed 29 Dec. 2018).

[57] Russia was reported to have deployed several electronic warfare capabilities in Syria for jamming airborne radars, for jamming unmanned aerial vehicles, and for jamming ground systems for mobile communications (GSM). See, McDermott, N. R. (2017), *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*, Tallinn: International Centre for Defence and Security, p. 13.

[58] McDermott, N. R. (2017), *Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum*, p. v.

[59] The US Department of Defense defines mission assurance as '[a] process to protect or ensure the continued function and resilience of capabilities and assets – including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains – critical to the performance of DoD [mission-essential functions]': see US Department of Defense (2012), *Mission Assurance Strategy*, Washington, DC: Deputy Secretary of Defense, p. 1, https://policy.defense.gov/Portals/11/Documents/MA_Strategy_Final_7May12.pdf (accessed 14 Apr. 2019); Bigelow, B. (2017), 'Mission Assurance: Shifting the Focus of Cyber Defence', in Rõigas, H., Jakschis, R., Lindstr öm, L. and Minárik, T. (eds) (2017), *9th International Conference on Cyber Conflict: Defending the Core*, Tallinn: NATO CCD COE Publications, pp. 6–7, https://ccdcoe.org/uploads/2018/10/CyCon_2017_book.pdf (accessed 30 May 2019).

NATO space-dependent capabilities	**Potential impact from the loss of capabilities**
Intelligence, surveillance and reconnaissance (ISR)	• Interference to the ISR capability that leads to faulty assessment and response to threats. • NATO could lose the possibility to transmit ISR information over potential adversaries' territory. • Loss of situational awareness in peacetime and at times of conflict, resulting in faulty decision-making. • Loss of battlefield awareness for the commander, thus putting the desired operational objective in danger. • Manipulation of ISR data through spoofing attacks, which could cripple defensive systems by sending falsified or excess information to decision-makers.
Missile defence	• The loss of missile defence capabilities in peacetime due to cyberattacks would diminish situational awareness on ballistic missile launches in the world – reducing intelligence on when and where a missile is launched, and by whom. In times of conflict and warfare, losing this capability may result in unintentional escalation. • In times of conflict, such a loss will have strategic, operational and tactical consequences for NATO missions and operations. • Cyberattacks on missile defence could occur in the form of spoofing, thus deceiving the ballistic missile command system. • The inadequate interception of the upcoming ballistic missile may result with civilian casualties.
Communications	• Losing communication systems or receiving spoofed data, thus compromising the integrity of information received. • Decision-makers (including presidents, prime ministers and senior military cadres) may not be able to send the necessary orders down the chain of command. • Decisions based on faulty information may lead to escalation and decrease the threshold for conflict.
Space situational awareness	• Loss of control or destruction of satellite control systems through the targeting of those systems or of mission packages by cyberattacks. • Altering the orbit of the satellite or 'grilling' its solar cells by exposing it to high levels of ionizing radiation.[60] • Inability to detect, predict or assess space debris or its re-entry, which could impact on life. • Disruption of missions and all other space services, thus impacting on military operations and on human life.
Environmental monitoring	• Cyberattacks on weather systems or on environmental monitoring systems may cause problems in defence planning for an attack as the military rely on daily weather information to conduct its operations. • Weather information is fundamental for land, air, and maritime domains. Cyberattacks on weather forecasting systems could impact on operational capacity.

[60] Livingstone and Lewis (2016), *Space, the Final Frontier for Cybersecurity?*

4. Capability Requirements

The NATO Defence Planning Process (NDPP) identifies capability needs. These requirements can be identified through following the DOTMLPF-I (doctrine, organization, training, materiel, leadership, personnel, facilities and interoperability) capability development approach, which is analysed in detail for space capabilities (see below).

Doctrine and policy

NATO needs to revise NATO concept, policy and doctrine to encompass the use of space systems and assets in military capabilities. While doctrine provides the main principles by which military forces shape and guide their actions, policy provides the 'prudent course of action or conduct to be applied in the application of a principle.'[61] NATO has not yet agreed on a space doctrine. Currently NATO is developing a comprehensive Space Policy, which is a positive outcome of the 2018 Brussels Summit.[62]

As every NATO operation requires and depends on space capabilities, it is a fundamental necessity to develop a space doctrine to guide operations. Below are some guidelines for the development of such a doctrine:

- Identify the objectives, threats and principles;
- Identify the level of ambition regarding the extent to which NATO wants (or does not want) to become an autonomous actor in space;
- Define cyber offensive and defensive capabilities of allies, and cyber defensive capabilities for NATO;
- Set out minimum capability requirements for satellite services, with consideration of non-survivability of assets and significance of redundancy; and
- Define the interaction with other organizations, including in the private sector and partnerships. The NATO Industry Cyber Partnership, launched in 2014, allows NATO to develop new concepts for technological advancement. The senior cadres should prioritize science and technology to a higher level in their agenda. The NATO–EU partnership is also important, particularly because the EU's Galileo navigational system could provide resilience to NATO systems.

[61] NATO (1997), *Logistics Handbook*, https://www.nato.int/docu/logi-en/1997/defini.htm (accessed 10 May 2019).
[62] NATO (2018), Brussels Summit Declaration, 11 July 2018, https://www.nato.int/cps/en/natohq/official_texts_156624.htm (accessed 10 May 2019).

Some of the issues cited above could be included in the forthcoming NATO Space Policy, rather than in a doctrine. For instance:

- A NATO Space Policy could identify the considerations of potential Article 5 incidents, which is the principle of collective defence. Cyberattacks that might disturb communications or destroy satellites are more likely to constitute part of a broader strategic campaign than an isolated incident. It is not the form a cyberattack takes, but the impact of such an attack that would lead NATO members to consider invoking Article 5.
- It is also worth acknowledging the geographical nature of Article 5. The North Atlantic Treaty (Washington Treaty) of 1949 states: 'The Parties agree that an armed attack against one or more of them in Europe and North America shall be considered an attack against them all […]'. There is an interpretational challenge to this, as cyberattacks are not bound by borders; moreover, they can be initiated outside Europe or North America but might have an indirect impact on those continents. The same applies to attacks on space assets, since they lie outside territorial boundaries. The NATO Space Policy will need to take into account a geography that includes the ownership of these assets and the geographical impact of any cyberattack on or through them.
- NATO's deterrence and defence policy involves ballistic missile defence (BMD), including interceptors, radars and the Active Layered Theatre Ballistic Missile Defence (ALTBMD) capability, which is a single battle management network that integrates all theatre ballistic missile systems, such as the Patriot missiles,[63] the SAMP-T system,[64] and the Medium Extended Air Defense System.[65] Cybersecurity considerations should include space technology that is used within the BMD capability.

While developing capabilities through doctrine and policies, legal considerations also play a significant role. In the Wales Summit Declaration of September 2014, NATO leaders agreed that a cyberattack could trigger Article 5 (to be assessed on a case-by-case basis) and that cyber domain was a valid operational area (similar to air, sea and land). In principle, by extension, cyberattacks on space systems may fall within this framework. The main question is whether a cyberattack on a space system's software without kinetic consequences might be considered as an armed attack that could trigger Article 5, or whether there must be direct or indirect kinetic consequences (such as the destruction of a satellite resulting in debris).[66] There is also the question of the application of international humanitarian law (IHL). NATO has stated repeatedly that international law and IHL apply in cyberspace. The *Tallinn Manual*, a non-binding advisory document,[67] also affirms the applicability of IHL to cyberspace. However, there are questions over differentiating cyberattacks against military objectives versus cyberattacks on civilian infrastructure, and over the assessment

[63] Patriot missiles were originally developed by the US and purchased within the NATO alliance. As stated above, Patriot is a long-range air defence system. It protects against tactical ballistic missiles, cruise missiles and advanced aircraft. See Army Technology (n.d.), 'Patriot Missile Long- Range Air-Defence System', https://www.army-technology.com/projects/patriot/ (accessed 10 May 2019).

[64] SAMP-T is a medium-range air defence system, produced by France and Italy. The aim of SAMP-T is to provide protection against unmanned vehicles, cruise missiles and short-range ballistic missiles (up to 600 km). It gives NATO an advantage in an anti-access/area-denial environment (A2/D2), See Missile Defence Advocacy Alliance (2018), 'SAMP/T Air Defence System (France & Italy)', http://missiledefenseadvocacy.org/missile-defense-systems-2/allied-air-and-missile-defense-systems/allied-intercept-systems-coming-soon/sampt-air-defense-system/ (accessed 10 May 2019).

[65] The Medium Extended Air Defense System was developed by Lockheed Martin, and it protects against tactical ballistic missiles (including nuclear-tipped ballistic missiles), unmanned aerial systems, cruise missiles and aircraft. See Lockheed Martin (n.d.), 'Medium Extended Air Defense System: About', https://www.lockheedmartin.com/en-us/products/meads.html (accessed 10 May 2019); NATO (2005), 'Launch of NATO's Active Layered Theatre Ballistic Missile Defence (ALTBMD) Programme', press release, 16 March 2005, https://www.nato.int/cps/en/natolive/news_21656.htm (accessed 10 May 2019).

[66] The author would like to acknowledge that Yasmin Afinam, research assistant at Chatham House, raised this point.

[67] Schmitt, M. (ed) (2013), Tallinn Manual on the International Law Applicable to Cyber Warfare, prepared by the International Group of Experts at the Invitation of Cooperative Cyber Defence Centre of Excellence, Cambridge University Press, Cambridge, csef.ru/media/articles/3990/3990.pdf (accessed 30 May 2019).

of the proportionality of a cyberattack prior to its execution. Realizing that civil and military assets are interlinked to a large extent, it is hard to estimate whether an attack is proportionate or not. Discussions with experts and NATO officials indicate that any Article 5 consideration would depend on the severity, consequences and political circumstances of an attack.

In future the use of emerging technologies, which includes AI, quantum-based cryptography, quantum computing and the development of space-based internet infrastructure, will define the future of warfare.

In future the use of emerging technologies, which includes AI, quantum-based cryptography, quantum computing and the development of space-based internet infrastructure, will define the future of warfare. Finding ways to transfer all necessary civilian capability to the military area with appropriate security measures could improve NATO’s capabilities, and incorporating a forward-looking approach to its doctrine and policies would benefit NATO in the long run.

Organization

Based on open-source analysis and on information shared among the members of the alliance, NATO is already mapping out the space capabilities of its allies. This will help assess both NATO’s existing resources and those that will be required. How quickly NATO can be fully operational in times of conflict and warfare and whether space is integrated into the planning structure are both important issues.

At the organizational level, the following considerations apply:

- The expertise on space technology rests with the private, public and military sectors. Strengthening the relationship across these three sectors would improve NATO’s organizational capacity.
- Although the cyber domain and space are intrinsically interlinked with each other, day-to-day tasks may hinder the development of common strategies by military staff. At the organizational level, there is compartmentalization. Increasing the coordination between the space and cyber communities would help to break down ‘silos’ (or barriers), and personnel could be trained in multifaceted skills.
- NATO could consider establishing new frameworks with the European Space Agency. One such framework that has already come under discussion includes the possible use of GNSS in military operations.

Training

Training is essential to create awareness and prepare the alliance for worst case scenarios. NATO could promote different types of training that would capture space security and system vulnerabilities to cyberattacks. Training areas could be selected through a lessons-learned analysis where former cases could be used to highlight areas of greatest need.

Some examples are as follows:

- At the political-strategic level, crisis management exercises (CMX), hybrid warfare exercises and similar training could incorporate cyber resilience and bring space elements into cybersecurity training.
- At the technical level, given the complexity of space systems, focused training, modelling and simulation would be key to ensuring design integrity.
- Bringing the technical and political communities together in training modules would be helpful. Often the political community and technical community do not metaphorically speak the same language and their concerns do not merge. Such training would be technology-driven and could incorporate modelling and simulation. Thus, technical expertise and knowledge could be transferred into political action plans.
- Training may also involve the private sector or contractors. NATO decides whether or not it should delegate parts of the training to the private sector or to conduct it internally. There are advantages and disadvantages in both. One of the advantages in delegating the work to an outside party is that the latter could conduct an analysis without any NATO restrictions and could significantly test NATO's planning and operations. The main disadvantage is that NATO may not be able to share classified information, which would make the training less comprehensive.
- Some of the most useful training methods involve exercises, 'war gaming', crisis simulations and scenario planning, as well as online training education programmes, training manuals, and certifications. NATO should also measure the impact of the training and assess its skill-maintenance capacity.

Materiel

Materiel involves military equipment and tools that could support the decision-making and operational planning entailed in considerations of the space-based systems sector. It also involves logistics and supply chain management, and the integration of cybersecurity system design into the mainstream development and design of space systems. Analysing which companies are habitually relied upon in the supply of satellite systems may help NATO allies to prioritize their supply chain security efforts. Software vendors have control over putting 'back-doors' in the system that may not be visible or known during the procurement stage. Requesting the establishment of security requirements at the design stage of a hardware project may also increase resilience and form part of a defence-in-depth strategy.

Additional points to be considered with regards to materiel may include the following:

- Should NATO have some sort of space capability, and, if so, what should the minimum capability be? Historically, NATO owned SATCOM capability, but political considerations led to the decision to rely instead upon the capabilities of alliance member states. To date, some countries within the alliance have not shown sufficient interest in NATO having its own satellite capability, and there has been no appetite to return to the old system.
- It is necessary to find approaches to incorporate EU assets and equipment into NATO capability in order to increase redundancy.

Leadership

Leadership considerations involve awareness, education and training in the vulnerabilities of strategic systems to cyberattacks; leadership capabilities should also cover the issue of the defence sector's interdependency with other sectors while conducting its operations. For instance, the telecommunications and defence sectors both use commercial space assets. The mutual dependency between the defence sector and other critical national infrastructure is particularly important in understanding the possible consequences of a cyberattack across all sectors.

Possible ways to improve leadership-level involvement may include:

- Conducting non-technical training for the North Atlantic Council (NAC) on space security. This type of training could also be conducted with NATO's Military Committee and Supreme Commanders.
- The establishment of a high-level scientific board comprising the chief scientific advisers to NATO senior cadres. This group could distil any technical information to the political group.

Personnel and facilities

Member states assign personnel to operate the NATO defence and military systems that are dependent on space assets. Allies may also choose to deploy space support teams to the conflict zone (such as those deployed in Afghanistan by France and the US).[68]

The qualifications of personnel can be improved by:

- Establishing personnel requirements for teams working on space issues.
- Creating incentives for career promotion and retention of skills in order to improve resilience.
- Creating memoranda of understanding with the private sector to set up joint work environments and establish hiring programmes where personnel with security clearances would be working at NATO through private-sector engagement.[69]
- Finding ways to convince the member states to send highly qualified personnel to NATO as nations bid to fill these posts. Creating minimum requirements for the bidding process would help to attract personnel with the right qualifications.
- As with the model followed by Estonia in the cyber domain,[70] it is critical for alliance countries to start investing in programmes of academic study on space technology, including at masters level, through which NATO personnel can receive training and certification. Such programmes will equip personnel with essential skills and provide the alliance member states with qualified assets.

[68] NATO (2013), *NATO Space Handbook*.
[69] There will be certain classification limitations that need to be handled accordingly.
[70] After the 2007 cyberattack campaign in Estonia that lasted for 22 days, the Estonian government invested in cybersecurity measures across its critical sectors, incorporated education and training in university curriculums and established NATO Cooperative Cyber Defence Center of Excellence in Tallinn.

Interoperability

Interoperability enables allies to operate their space systems without having to make adaptations so that their systems can function efficiently.

Interoperability has been an issue in the land, air, and maritime domains. Space-assets planning would benefit from the lessons learned in those domains – for instance, by studying and understanding the complexities involved in intelligence- and information-sharing across all domains. Allies could allocate funds towards a body of work that could focus on interoperability in space. Doctrines and standardization could help to improve interoperability among allied systems. Yet, allies should also realize that standardization would mean using the same vectors as a baseline, thus leading to an increase in risk (in the remaining vulnerabilities) across the alliance as a whole.

> Allies should realize that standardization would mean using the same vectors as a baseline, thus leading to an increase in risk across the alliance as a whole.

In order to share secure information through SATCOM units, France, Germany, Norway and the US have formed the multilateral Coalition Network for Secure Information Sharing (CoNSIS). Through secure communications systems, CoNSIS’s objective is to enable better and more accurate decision-making, within a shorter period of time.[71] In order to ease interoperability, CoNSIS uses commercial standards as its baseline.[72] For future applications, it is advisable to check whether commercial standards meet cybersecurity demands for military requirements.

Interoperability in technology is desirable but remains a challenging construct. It could become the role of NATO to make national space services interoperable. Creating a catalogue of national services might be a good starting point. Interoperability could also be established at the product level (for example, in the field of space weather information) where the products are standardized across the alliance. In order to incentivize nations to invest in this endeavour, it might be helpful to calculate the cost of inadequate interoperability across the alliance to demonstrate current or potential monetary losses.

[71] CoNSIS – Coalition Networks for Secure Information Sharing (n.d.), https://www.consis.info/ (accessed 10 May 2019).

[72] Ibid.

5. Recommendations and Observations

Some of the recommendations and observations suggested below are activities that are currently in the planning stage – as part of the NATO Space Working Group Action Plan, or as part of ongoing discussions with allies. However, these activities have not yet been implemented and require continuous attention.

- Encouraging allied member countries to be responsible for protecting their own space capabilities, and to consider space in national force structures rather than in the NATO command structure. In addition, NATO should consider how the configuration for space assets between the allies and NATO would look in time of conflict.
- There is a need for a NATO Centre of Excellence (CoE) for space. In cyberspace, the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) shares information between NATO, the allies and NATO partner countries. However, the alliance lacks an established CoE for space policy.
- NATO is trying to link national space operational centres (to date, these include those of the UK and Canada) in order to establish routine contact and for regular information-sharing. It would be valuable to incorporate all allies that have space capabilities into this initiative; and to start discussions with allies that have space aspirations.
- NATO lacks a 24/7 operational cell that can observe and monitor activities relating to space. It could create a space coordination cell, in order to coordinate knowledge and data in all of the six capability areas outlined in this paper.
- Further planning needs to go into the integration of new technologies when securing satellites from cyberattack. Aspirations in this area may include the ability for satellites to configure and fix themselves.
- A NATO Industrial Advisory Group (NIAG) study is required in order to examine ways of sharing information between NATO and the private sector. Through this study, NIAG could provide industry advice to the Conference of National Armaments Directors and to other NATO units. Such advice could shape NATO military capability requirements and be linked to the next cycle of the NDPP.
- Current cybersecurity maturity standards and guidelines (such as those published by the US National Institute of Standards and Technology) help organizations to improve their cybersecurity measures and best practices. How effectively cybersecurity maturity standards can be applied to space-sector maturity should be analysed further. If the two areas are different in essence, then separate standards and guidelines for space could be developed.
- Securing space assets against cyberattacks at the design stage is particularly important, and should be a fundamental component of satellite and ground station design from the initial concept – giving rise to a 'security-by-design' approach.
- Information Sharing and Analysis Centers (ISACs) help improve collaboration and resilience in the cyber realm. Similar types of national centres in the space sector could provide insights and could improve engagement between allies.

- The annual NATO Information Assurance Symposium (NIAS) Cyber Security Symposium could focus on space in upcoming years.
- The potential establishment of a NATO science and technology committee, involving or led by the NATO Communications and Information Agency (NCI Agency), could be further explored. Such a committee could be relied upon to give advice on relevant cyberthreats and vulnerabilities, such as those related to the integrity or security of supply chains.
- The NCI Agency is responsible for operating and defending NATO's networks, and rapid sharing of information has proved to be one of the most effective defences in cyberspace. In the cyber domain, there are certain tools in place – such as the Malware Information Sharing Platform (MISP) – that promote cooperation and information-sharing among allies. Information-sharing could also be more closely examined in relation to the space sector. Through sharing information and explanations of operational impact, NATO could increase allies' awareness with regards to space-based threats.
- NATO should further increase its efforts to strengthen its cyberdefence posture through the NATO Industry Cyber Partnership: enhancing collaboration between the public and private sectors is one of the fastest and least expensive ways to increase cyber resilience, improve incident handling and mitigate vulnerability to attack. Moreover, this should foster timely information-sharing on cyberthreats, allowing stakeholders to enhance situational awareness and better protect their networks. In practice, for instance, it should facilitate rapid and early bilateral exchange of non-classified technical information related to cyberthreats and vulnerabilities. Improvements in the cyber domain would have a positive impact on the space realm.
- Under a future NATO Space Policy, defence planners should define NATO's space capability requirements and present them to all allies by means of the NDPP.[73]
- NATO Space Policy could lead to recognizing space as the fifth domain. This would help NATO better plan for future operations that use space assets and technology and to incorporate space into the defence planning structure.
- Increasing awareness at all levels require holistic exercises and tests in order to give end users experience in how these systems actually work. Therefore, space considerations should be incorporated into existing exercises and training.
- The entanglement between commercial and military space assets may also cause vulnerabilities. In future, military systems will be increasingly connected to non-military systems. This has important implications for the laws of armed conflict, as the combination of civilian, commercial and military capabilities in the cyber domain and space raises the risk that civilian capabilities used for military purposes qualify as legitimate military targets.
- NATO should ensure that contractors that rely on commercial standards follow minimum cybersecurity arrangements.
- NATO may consider ensuring that commercial contracts meet military protection standards, in order to mitigate the risk posed by the military's use of commercial space assets.

[73] Fleischer, P. (2016), 'Above the Moon: NATO Space Policy', http://futurenato.org/articles/above-the-moon-nato-space-policy/ (accessed 28 Nov. 2018).

- NATO should conduct a gap analysis that will identify the following: which countries NATO relies upon for space services; what type of capabilities these countries possess; what type of capabilities they should have for future warfare; and what actions NATO needs to take (the latter being subsequently enshrined in an action plan).

- Although NATO does not lead development of the space sector and it is the allies that provide space capabilities, NATO can still initiate informal discussions with the allies on the establishment of targets for space resilience. In the cyber realm, for instance, cybersecurity targets have been incorporated into the NDPP.

- Mapping out recurring threats to space systems and promoting standardization to address common weaknesses may increase resilience. If standardization is unwanted due to its risks, then a voluntary 'best practice' approach can be utilized. NATO's military command may also enter into direct discussions with the allies to set up minimum requirements. In this regard, a commanders' intent paper can also capture space infrastructure.

6. Conclusion

This paper addresses the subject of potential vulnerabilities of space-dependent strategic systems to cyberattacks. With the awareness that NATO and the NCI Agency are already working on protecting NATO's space-dependent systems, this paper has provided complementary analysis and insights regarding the issues at stake.

Today, norms around space security are considered lax: this also applies to those around cybersecurity. The Manual on International Law Applicable to Military Uses of Outer Space (MILAMOS), which is similar in scope to the *Tallinn Manual* (see above), was launched in 2016 through a civil society initiative, aiming to clarify the rules applicable to the military use of outer space.[74] The United Nations has appointed GGEs on cyber and space developments. Unfortunately, the most recent space GGE failed to reach agreement (not in itself an uncommon occurrence for either group in their successive forms).[75] It is imperative to create ongoing efforts and synergy between the cyber GGE and space GGE. Establishing norms of secure cyberspace would also improve space security.

It is important to realize that the conduct of warfare has changed drastically in the 21st century. The definition of peacetime and conflict time activities is becoming increasingly blurred. There is no consensus on how to interpret attacks on space-based systems or on cyber networks, whether in crisis or in peacetime.

Russia continuously tests NATO's maritime and air domains in multiple geographies, including through space means. Deciding on what would be the threshold of hostile intent in space could help to synchronize efforts among NATO allies. Moreover, NATO's defence posture cannot only rely on how to win the next conflict or how to manage vulnerabilities: it should make sure that threats do not materialize through effective deterrence postures.

NATO has not yet defined space as a domain, though some allies recognize it as such. Current political structures at NATO, however, err on the side of caution, and it is claimed that NATO will recognize space as a domain in the upcoming London Summit.[76] After the adoption of the Space Policy, perhaps there would be a window of opportunity to define space as a domain. It could kick off a future study on what constitutes such a domain, what type of similarities and divergence cyber shares with space, and whether a similar approach could be modelled for space. For instance, if NATO declares space as a domain, it could create a joint Bilateral Strategic Commands (Bi-SC) – NATO Allied Command Transformation and NATO Allied Command Operations – vision of space. A Bi-SC vision would set out minimum requirements, conduct capability analysis, and assess collective assets *vis-à-vis* the command structure.

[74] McGill University Institute of Air & Space Law (n.d.), https://www.mcgill.ca/iasl/milamos (accessed 10 May 2019).
[75] The draft report of the space GGE was made public as an annex to the following working paper submitted by Nigeria on behalf of the UN African Group: see UN Disarmament Commission (2019), 'Recommendations to promote the practical implementation of transparency and confidence-building measures in outer space activities with the goal of preventing an arms race in outer space, in accordance with the recommendations set out in the report of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities', Working Paper A/CN.10/2019/WP/1, https://digitallibrary.un.org/record/3801525 (accessed 10 May 2019).
[76] Emmott, R. (2019), 'Exclusive - NATO aims to make space new frontier in defence', Reuters, 21 June 2019, https://uk.reuters.com/article/uk-nato-space-exclusive/exclusive-nato-aims-to-make-space-new-frontier-in-defence-idUKKCN1TM17F (accessed 27 Jun. 2019).

Protection of critical national infrastructure would not only improve civilian preparedness and resilience: it would also help to minimize impacts on the military sector. The NATO Pipeline System, for instance, that NATO forces rely on for refuelling and storage, uses a command and control structure to link 'storage depots, military air bases, civilian airports, pumping stations, truck and rail loading stations, refineries and entry/discharge points.'[77] This command and control structure relies on civilian ground and satellite communications; hence there is reliance on the GPS/GNSS systems. As a result, the security of civilian sectors is directly linked with protecting military objectives. The EU, for instance, budgeted €6.5 billion to support dual-use infrastructure for the transportation sector, with the aim of adapting Europe's transportation sector to military requirements.[78] Inclusion of the space element in existing infrastructure considerations within the EU could help improve resilience.

An assessment of the extent to which NATO can access Galileo – the EU global satellite-based navigation system – and what such a configuration would look like, would be helpful for protecting operations. NATO should also consider how space technology could strengthen deterrence postures, ensuring that serious threats would not materialize at times of crisis.

If capabilities remain in national hands NATO's role in the space realm should be considered. It could have the following functions:

1. Intelligence;
2. Creating dialogue with the space components industry;
3. Operational planning; and
4. Coordination/liaison with the allies on personnel requirements, in order to improve alliance knowledge and capacity on the use of space technology in NATO operations.

In many areas, NATO allies that have either not invested in space technology or do not have sufficient capability to protect their systems, look to NATO as an informative entity that could guide them towards the best approach for space security. If NATO's role in the space realm were to be clarified as discussed above, this could help those allies to perform their obligations.

NATO's level of ambition for defence is to be able to have real-time Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR) capability in all four domains. Protection of space services should be at the core of this ambition.

Today, commercial ISR capabilities rival military capabilities. Thus, working effectively with industry to ameliorate and strengthen ISR capabilities, and seeking out innovation in a cross-disciplinary environment, would help NATO to project its power and improve its response speed to threats. The industry could also be held accountable in case of cyber breaches and potential misconduct. Industry could also play a fundamental role in incorporating safe and secure technologies into the space realm.

It is clear that human societies are dependent on space, but it is less clear how to mitigate cyber risks and protect space assets. To improve resilience, those designing mitigation measures should consider:

1. Technological aspects, such as incorporating terrestrial back-ups for guidance systems, or investing in quantum systems for secure communication.

[77] NATO (2017), 'NATO Pipeline System', https://www.nato.int/cps/en/natohq/topics_56600.htm (accessed 10 May 2019).
[78] European Commission (2018), 'EU Budget: Commission proposes increased funding to invest in connecting Europeans with high-performance infrastructure', press release, 6 June 2018, http://europa.eu/rapid/press-release_IP-18-4029_en.htm (accessed 10 May 2019).

2. The value of investing in assurance/redundancy systems.
3. Recovery capacity, including how quickly a system could be fixed or what type of forensic applications may help to aide attribution problems, how quickly NATO could achieve full operational readiness, and so forth.
4. Organizational culture and human resources aspects, such as training and education and human-in/on-the-loop considerations,[79] while incorporating emerging technologies, especially artificial intelligence.

[79] Human in/on the loop is a concept that explains human-machine interaction and the role of humans and human control in (semi) autonomous systems.

About the Author

Dr Beyza Unal is a senior research fellow with the International Security Department at Chatham House. She specializes in nuclear and cyber policies, conducting research on cybersecurity and critical national infrastructure security and cybersecurity of nuclear weapons systems. Dr Unal also conducts research on urban preparedness and city resilience against CBRN threats.

She formerly worked in the Strategic Analysis Branch at NATO Allied Command and Transformation, taught international relations, transcribed interviews on Turkish political history, and served as an international election observer during the 2010 Iraqi parliamentary elections.

Dr Unal is interested in NATO’s defence and security policy as well as security in the Middle East, and has been given various fellowships for her achievements; most notably, she is a William J. Fulbright alumna.

She has also received funding from the US Department of Energy to participate in workshops in Brookhaven National Laboratory, the James Martin Centre for Nonproliferation Studies, and Sandia National Laboratory.

Acknowledgments

The author would like to thank the Norwegian Ministry of Defence for their funding and support of this research project. In particular, the active engagement of Jamie Shea, University of Exeter; Xavier Pasco, Fondation pour la Recherche Strategique; Audun Jøsang, University of Oslo; and Barbara Angelucci, Rhea Group, has been instrumental.

The programme is also grateful to Marco Macori and Guido Gluschke from Brandenburg University of Applied Sciences, for their valuable comments during the preparation of the two meetings commencing this report. Also, thanks go to Bleddyn Bowen, University of Leicester; Ali Stickings, Rusi; Daniel Porras, United Nations Institute for Disarmament Research; and Steinar Høibråten, Norwegian Defence Research Establishment (FFI). In addition, the International Security Programme at Chatham House played a key role in the development of the research project meetings, including David Livingstone, associate fellow; Patricia Lewis, research director; Yasmin Afina, research assistant; and Calum Inverarity, programme coordinator. Finally, thanks to all the contributors to this report, to the peer-reviewers, as well as the participants who took part in the seminar discussions.

Independent thinking since 1920

Chatham House, the Royal Institute of International Affairs, is a world-leading policy institute based in London. Our mission is to help governments and societies build a sustainably secure, prosperous and just world.

Chatham House does not express opinions of its own. The opinions expressed in this publication are the responsibility of the author(s).

Cover image: The radar domes of RAF Menwith Hill, reported to be the biggest spy base in the world, dominate the skyline on 30 October 2007, in Harrogate, UK.

Photo credit: Copyright © Photographer/Getty Images

ISBN 978 1 78413 340 5

The Royal Institute of International Affairs
Chatham House
10 St James's Square, London SW1Y 4LE
T +44 (0)20 7957 5700 F +44 (0)20 7957 5710
contact@chathamhouse.org www.chathamhouse.org

Charity Registration Number: 208223