Article

The North Atlantic Space Schism and the Ambiguity Problem: NATO's Collective Space Defence Posture

By Scott Mackie

Biography: Scott Mackie received an MA (Hons) in Politics and International Relations from the University of Aberdeen in 2012 prior to serving as a Surface Warfare Officer in the Royal Navy. He is currently reading for the degree of Master of Research at the University of Portsmouth and his main research interests are UK and NATO space policy, as well as issues surrounding space capability, expectations, and ambition.

Abstract: As NATO seeks to integrate space as an operational domain, a schism between the US and the remainder has emerged as to how best to operate in space. Is it sufficient to merely operate through the domain - to support and enable operations? Or is it necessary to command the domain - to operate in, from and through. NATO's approach to space lacks maturity, and attempts to treat the integration of space as it has with the traditional domains are insufficient. As a result, NATO's collective approach to operations and security in space are reactive rather than visionary.

Introduction

Space is the next frontier in human exploration, and like all frontiers it must be safeguarded to ensure supremacy and survival. It is the environment on which modern communications, the global positioning system, internet connectivity, and a broad spectrum of warfighting capabilities depend. Sixty years after the collective effort that landed man on the moon – a period in which our reliance on space has increased exponentially - the domain is once again the subject of increased attention, and particularly so amongst the members of the North Atlantic Treaty Organisation (NATO). Yet despite the importance of space infrastructure and the recognised need to protect it, the publication of new defence space policies,[1] and the formation of new national space commands,[2] NATO's collective space posture lacks clarity. Ambiguity permeates its approach to security in space, hampering not only the ability of member nations to effectively exercise their inherent right to self-defence which extends into the space domain, but also the ability of the Alliance to execute its core function of collective defence and security.

This lack of clarity is centred on four areas. The first area concerns the unique positioning of NATO within the security apparatus of the North Atlantic area: the challenges posed by a 30-member alliance, and the adaptation that the Alliance must undertake as it enters, arguably, its third era of adaptation with the accession of the space and cyber environments. In the second area, the size of the threat continuum poses a particular problem for decision makers: in an arsenal that includes conventional strikes against ground-based components, complex cyber-attacks against digital infrastructure, and direct kinetic strikes against orbital assets, how does NATO ensure that it has the capability and resource to defend against all threats? This is compounded by questions over approaches to governance and how these are impacted upon by national policies. Thirdly, the distinction between space as a warfighting or operational domain coupled with an increasing divergence over national approaches to the use and governance of space. Nations are declaring how they will operate in space - their ambitions and their limitations - according to traditional approaches. The warfighting domain is the domain where offensive, defensive *and* enabling military operations occur, and it is this concept that underwrites the spaceward efforts of the United States (US), Russia and China. The operational domain, meanwhile, is a 'discrete sphere of military activity within which operations are undertaken to achieve objectives in *support* [author emphasis] of the mission'.[3] These definitions - the traditional strategic orthodoxy of securing, operating within, and commanding the physical domains of land, sea, and air - are sufficient, for the new global commons is, despite best efforts, inappropriate. The fourth and final area concerns whether the North Atlantic Treaty and NATO's approach to the domain facilitates and supports a credible and robust responsive space posture in an era defined by increased commercial partnerships and amplified inter-state competition. It focuses on the idea that the new global commons cannot be secured according to the 'old' principles of collective defence that have defined NATO's security posture for over 70 years. It seeks to address the question as to whether the Alliance could realistically invoke Article V in response to an attack on its space

infrastructure, whether it would be appropriate for it to respond, and whether it could credibly do so.

This paper will therefore examine NATO's adaptation to its new operating environments, and its attempts to generate a collective approach to space security. This will be framed through the perspectives, actions, and policies of the United States (US), of European members including the United Kingdom (UK), France, and Germany, and with particular regard to the continually diverse range of counterspace threats emerging from hostile actors, especially Russia and China. It will also assess differing approaches to space operations, space priorities, whether they are prepared to use force in defence of space infrastructure, and their relationship with the existing and developing governance of space in the twenty-first century, demonstrating an inherent link between individual national and collective attitudes towards governance and approaches to security in space. The third section examines the nuances of collective defence - the North Atlantic Treaty, geographic boundaries, and traditional responses. It will also look at the threshold conundrum that exists in the new global commons, exacerbated by the challenges to response posed by dual-use satellite technologies, before discussing whether the ambiguity surrounding collective defence is deliberate or accidental, and how this precludes the Alliance from responding in a credible manner in space.

NATO, Space, and the Third Era of Adaptation

Whilst the challenges posed by operating in space are not unique to NATO, the way in which it approaches security issues is. Unique to NATO is the all-encompassing nature of its defence posture, and the importance and centrality with which individual governments afford their membership of and participation in the Alliance in their national strategies. This, coupled with the fact that NATO continues to grow its membership, and with the substantial range of security issues it has committed itself to address, makes it a potentially powerful collaborative actor in the space environment.[4] More members arguably generate more capacity, contribute to a more robust collective capability portfolio, and invariably increase the amount of coercive power (political, diplomatic, economic, and military) that is available to be brought to bear against an adversary, as well as reducing the overall cost to individual nations in terms of gold and manpower. This burden sharing allows individual nations to develop strength *in depth*, but at the cost of strength *in breadth*: that is to say, they can often specialise in specific areas such as air defence, mine countermeasures or anti-submarine warfare, but often at the expense of other areas, relying on others to provide capability in that particular area. It also creates more opportunities for divergence in approach due to conflicting security priorities. Do burden and capability sharing offer a route for the Alliance to achieve supremacy in the space environment: sharing resource and responsibility across the broad spectrum of space capabilities?

Space is by its very nature different: it is global and all-encompassing, with no national distinction or claim, and is not easily accessed without specialist equipment and knowledge. It must therefore be treated as different, and this can only be achieved with a fundamental shift

in the way that security in space is approached. The challenge of adapting to a new strategic environment is not new to the Alliance: NATO has continually had to redefine its role and re-affirm its relevance in a post-Cold War operating environment defined by hybrid, asymmetric and unconventional warfare, whilst simultaneously maintaining its core function as a collective defence alliance. This process of adaptation has been the subject of frequent academic scrutiny, and Thierry Tardy notes that 'adaptation policies over the last decade have created such adverse effects and costs that may increase NATO's vulnerability rather than strengthen its relevance' and that 'to focus on a narrow military segment, or to broaden too much its security agenda would be examples of maladaptation'.[5] Tardy identifies two distinct period of transition for the Alliance: the early 1990s and 2000s when 'crisis management' formed a core function of the Alliance, and in the mid to late 2000s and early 2010s when counter-terrorism operations were the defining characteristic. Might it now be that NATO has entered a third era of adaptation as it attempts to find its way in the all-encompassing global commons? It is on this basis, presumably, that space has been included as collective defence issues: indeed, Tardy suggests that, as the nature of the threat has evolved, the 'appropriateness of narrow defence' and the 'centrality of collective defence' [6] are now inevitable questions that must be asked of the Alliance and its approach. Is space an environment where NATO can realistically adapt and exercise its core security functions?

NATO, as it attempts to embrace the era of the new global commons and the increasing requirement for integrated multi-domain operations, is faced with the challenge of adapting its existing architecture to ensure that its collective security posture credibly extends into the space domain. The outcome thus far has been simultaneously contradictory: bold and lacklustre, and visionary whilst lacking clarity. It is this lack of clarity and the resultant ambiguity that represents the greatest danger to the alliance and its security in the space domain.

The Growing Threat and Capability Spectrum

A single satellite launch changed the trajectory of the Cold War and of NATO. When the Soviet Union launched Sputnik I on 4 October 1957, the eight-year-old Alliance was already focused spaceward: two months previously the Soviets had declared their first inter-continental ballistic missile - the R-7 Semyorka - fully operational.[7] The militarisation of space had begun and it offered a unique environment from which to watch, to support operations, and to detect and react to emergent situations. Since then, space has been a constant companion to the development and conduct of warfare, though its status as a theatre of operations has, until recently, been hampered by technological limitations and a relative disinterest by national governments who were - for a period - content to rely on major space-faring allies (namely, the US) for the provision of expensive space-based functionality, freeing up their own funds for conventional defence programmes, or to fund other domestic priorities.

NATO highlights the challenges of developing threats throughout its narrative, and noted in its 2022 Strategic Concept that: 'Strategic competitors and potential adversaries are investing in technologies that could restrict our access and freedom to operate in space, degrade our

space capabilities, target our civilian and military infrastructure, impair our defence and harm our security'.[8] The US Defence Intelligence Agency (DIA), in its 2022 assessment of threats to US space capabilities, presents a much more detailed analysis of the counterspace threat continuum,[9] and highlights the broad range of threats and capabilities possessed by an increasing number of hostile state-actors. These threats range from the reversible (such as denial and deception of satellite functions and capabilities), to the irreversible (kinetic attacks on ground or space infrastructure, or a nuclear detonation in space). Russia and China in particular are identified as having invested significant resource and capital into their space and cyber programmes and have grown their combined operational space capability by seventy per cent,[10] developing extensive space surveillance networks, and technologies designed to deny opponents use of and access to space. Reversible action is the likely plan for any aggressor, such as the denial of GPS in an area of contention, or the temporary interference of communications signals between allied units in a contested area - actions which could be highly effective and limit operational effectiveness of units, and which are increasingly difficult to attribute.

The most significant threat comes from weapons within the irreversible threat arena, particularly in the form of kinetic strike weapons. Such attacks are likely to be orchestrated against terrestrial ground-based targets such as satellite uplink facilities or cyber command and control systems. These attacks are more likely because they rely not on specialist space-based weaponry, but on 'traditional', affordable, and widely available and tested conventional weapon systems. In terms of prosecuting orbital targets, direct-ascent anti-satellite (DA-ASAT) missiles designed to target and destroy satellites are of particular concern, and are a capability that has been successfully demonstrated by the US, Russia, China, and India.[11] Despite the risk that these weapons pose, Joan Johnson-Freese and David Burbach note the development of this technology [DA-ASAT] has been 'deemed politically acceptable' by viewing DA-ASAT development as an extension of ground-based missile defence, under the auspices of a country's right to self-defence.[12] This threat is of concern not only because of the devasting impact they can have on assets in space, but also due to the second and third order effects of an impact or collision. In each of the tests conducted, substantial debris was created in orbit as a result of impact, adding to the 27,000 pieces already tracked.[13] This in turn increases the danger to existing infrastructure: when satellites collide with even the smallest pieces of debris the results can be 'catastrophic'.[14]

The threat is not restricted to missiles: the development and deployment of satellites and platforms designed to inspect, maintain, and repair assets in orbit could also have a secondary use: rendezvous or proximity operations. Jürgen Scheffran identifies several ASAT roles a satellite could fulfil, including 'pushing targets off orbit, colliding with them, employing electronic jamming' or 'releasing destructive devices such as explosives, chemicals or radioactive materials'. [15] This 'co-orbital' threat further complicates the ability to protect space-infrastructure as this would represent a potentially offensive capability prepositioned in orbit. The UK - in its own submission to the UN - observes that its *Remove DEBRIS* satellite has

'proven harpooning capabilities'.[16] Whilst the capability has been developed for innocent use - to reduce the amount of debris in orbit, the UK alludes to potential military applications, noting that it 'could lead to concern or misunderstanding'. Benjamin Statts observes that the 'ambiguous nature [of satellites] makes it difficult to assess the user's intent at any given time [whether benign or aggressive]'.[17] And that is to say nothing of surplus or obsolete assets being used as 'kamikaze' satellites, used to maliciously impact other assets. A satellite does not have to be designated for military use to be a weapon.

Meanwhile, whilst their opponents advance their ability to strike kinetically *in* space (the capability to fight *in* the domain), NATO members have no comparable programmes in development - though Russia have stated that the US and its allies have been 'silent about their own efforts'.[18] In April 2022, the US publicly committed to cease destructive DA-ASAT missiles tests following a Russian test in November 2021, remarking that '[destructive tests] jeopardize the long-term sustainability of outer space and imperil the exploration and use of space by all nations'.[19] Whilst a noble sentiment, it can be viewed as just that: a sentiment. The US has already successfully demonstrated a credible offensive space capability through its use of modified anti-ballistic missile-defence technology to destroy an ageing US satellite in 2008.[20] This demonstration served a mission-specific purpose and was not the result of a dedicated offensive weapon development programme. This distinction was made clear by the US at the UN in 2008 when it stated that: 'The United States has no plans to adapt any technology from this extraordinary effort for use on any current or planned weapon system'.[21]

This position is not unique to the US: no other NATO member has indicated aspirations to develop offensive space capability, despite policies of proactively defending their space infrastructure. Nor is the US' commitment to abstain from destructive DA-ASAT testing unique: a number of Alliance members, including Germany, the UK, France and Canada, have followed the lead of the US and announced that they will not conduct destructive testing.[22] As it stands, none of the countries that have made this commitment have DA-ASAT testing programmes, but the unspoken nuance is that they will not *destructively* test such weapons - leaving scope for their future development or purchase nevertheless. How credible this would be remains to be seen: an untested or un-demonstrated capability cannot realistically constitute a credible response option, or a convincing deterrent.

Much attention is focused on the ability of the state to strike in space, and of the vulnerability of orbital assets. Less focus is perhaps afforded to the ground-based infrastructure and its vulnerability to 'traditional' kinetic assault, or the increasing threat that is achievable via cyber. The application of such attacks and their impact are beyond the scope of this paper, but it is important to recognise that orbital systems are critical components in the Alliances infrastructure and enable a wide range of military functions including the provision of secure communications networks, military GPS, reconnaissance satellites and the astro-inertial guidance systems that are a critical component of strategic nuclear weapons systems.

Whilst physical attacks on ground infrastructure are unlikely - they could be much more easily attributed to a perpetrator, and their legal status under the North Atlantic Treaty is much clearer - cyber-attacks on digital and space infrastructure are of increasing concern. Fortunately, cyber within NATO - at the operational and policy levels - is more doctrinally mature in comparison to its new global commons counterpart of space. That is not to say that efforts in the cyber domain alone are sufficient to deter aggressive action: they are undermined by a lack of visible deployment, and by the same attribution issues that plague the space environment. These challenges are compounded by the simple fact that traditional kinetic weapons and access to cyber space are much cheaper than space-borne weaponry, and more accessible to a wider range of state and non-state actors than ever before.

Much like the arsenal of weapons available, the threat origin has also expanded: whilst Russia has been the 'traditional' space-competitor to NATO, China has 'caught up' in recent years as it 'strives to subvert the rules-based international order, including in the space, cyber and maritime domains'.[23] The US 2022 *National Security Strategy* (NSS) recognises China as its 'most consequential geopolitical challenge',[24] though Pierre Haroche and Martin Quencez note that NATO has not yet designated China as a 'military adversary'.[25] Such recognition would require a shift in NATO's posture towards the Indo-Pacific: an act that many are reluctant to commit to in the face of Russian aggression on the Alliances eastern borders.[26] Unless policy is adapted to meet and challenge China's ambition in the near-term, NATO members will be forced to dedicate significant resource bridging any future capability gap to remain competitive and credible across all domains, particularly space.

Notwithstanding protestations against the testing and use of ASAT technology, and allusions to capabilities in documents, policies, and speeches, the fact that individual nations have not published exact details of their response plans and capabilities is not surprising: it would diminish any advantage they may possess over potential adversaries. There remains, however, a visible divergence in approach between the US and other Alliance members: the desire to use force *in* and *from* space (US), versus its principal utilisation to support operations across the other domains - to operate *through* space (the remainder). NATO cannot hope to have a coherent response to its adversaries in space if the policy approaches of its members are not in alignment. As the number of spaceward nations and commercial enterprises increases, so too does the likelihood of confusion and conflict.

Warfighting or Operational, and the Impact of Governance

Dolman observes that a domain 'cannot be commanded from an adjacent domain': it can only be contested.[27] In an environment where space is global and encompasses the air, land, and maritime domains,[28] how a nation defines its approach to space has implications for the development of capabilities and its response to threats. It follows that states must have a credible defensive and offensive posture *in* space: they must be able to 'fight in the domain, and *from* [author emphasis] the domain', as well as *through* the domain.[29] Command of space supports success and operational effectiveness across all domains: it is no coincidence that

the US, Russia, and China have all declared space as a warfighting domain, and that each has developed, or is developing, offensive space capabilities: the ability to fight *in*, and to retain and enforce their ability to fight *from* and *through*. Meanwhile, NATO – save the US – is tending towards operational and defensive support postures: the ability to support fighting elsewhere *through* the domain. Whilst multi-domain integration (MDI) programmes seek to address operations across domains, they are limited by traditional definitions: MDI in an operational context will look very different to those in a warfighting one, whereas the space environment requires an exclusive approach, tailored to its status as a unique battlespace where operational and warfighting are, fundamentally, one-and-the-same.

'Through, From and In' or 'Enable and Support'

Dolman describes the warfighting domain as one requiring 'specialised knowledge and training, unique tactics and doctrine, [and] a distinct operational perspective' with the objective to 'maximize combat power *within* and *from* [author emphasis] the domain',[30] and arguably *through* the domain. The US asserted in 2019 that 'space is the world's newest war-fighting domain'[31] – but it has always, in practice, acted as though it was a war-fighting domain. Steve Lambakis notes that the 1970s Strategic Defence Initiative was an attempt to secure US supremacy and ensure its ability to exercise its right to self-defence in space.[32] This commitment was echoed half a century later in the 2017 US NSS whereupon any 'harmful interference with, or attack' directed towards US space 'architecture' would be 'met with a deliberate response at a time, place, manner and domain of our choosing'.[33] This was reaffirmed in the 2020 *Defense Space Strategy* with an objective to 'maintain space superiority', with the requirement to 'protect and defend … space capabilities', and to 'deter and defeat adversary hostile use of space'.[34] It defined building a 'comprehensive military advantage in space' as a main line of effort, including the development of space warfighting expertise and the deployment of capabilities to counter its adversaries.[35]

This clarity of purpose is not without challenge: new administrations have new approaches, and the 2022 US NSS softens the approach towards the use of force and prioritises 'working with allies and partners' and the avoidance of 'destabilizing arms-races'.[36] This should not be taken as a weakening of resolve, but instead as the adoption of a more considered approach to limiting the militarisation of space in the long term. Alternatively, this could be a case of attempting to 'close the stable door once the horses have bolted' – attempting to limit arms development *after* the US has demonstrated credible offensive space capability, securing its own strategic advantage, or to limit its adversaries from attaining parity. Current policy notwithstanding, it highlights one of the key challenges faced by NATO: how does the Alliance generate a coherent response in the domain when individual members policies are subject to significant changes in approach?

NATO, meanwhile, declared space as an operational domain in 2019 and prioritised the integration of capabilities into the delivery of its 'core' tasks, including collective defence.[37] The Alliances efforts are focused on operational support, on coordination, and on the assessing

the impact of space on 'deterrence, defence and resilience'. Particular attention is afforded to space domain awareness (SDA), and to the role of space as a 'key enabler' for the other domains.[38] Underpinning these objectives is an admission that the Alliance is not 'aiming to become an autonomous space actor'. [39] This approach mirrors that of its other (non-US) spaceward members: France identifies support services, SDA, support to operations and 'active space defence' as its core priorities,[40] states its inherent right to self-defence and commits itself to acting in defence of its assets.[41] Germany has orientated its efforts towards SDA and provision of satellite capabilities,[42] whilst the UK's *Defence Space Strategy* also notes space as a 'key enabler' for its operations, and emphasises a focus on satellite communications (SATCOM), SDA and intelligence, surveillance and reconnaissance (ISR) development.[43] All three nations highlight the importance of interoperability and avoiding duplication of effort: of burden sharing and pooling capabilities.

The Absence of Cohesive Governance

The designations of space as warfighting or operational do not exist in isolation: approaches to military operations in space are an extension of a nation's overall attitude towards space and of its own priorities. Any approach is framed by legal obligations, and it is in these areas that NATO's membership appears more aligned. The principles to which a nation subscribes defines - and enables or restricts - its use of space, regardless of designation. This use is underpinned by a series of treaties, declarations, principles, conventions, rules, and norms, as well as an array of national legislation. Of the five treaties governing space, The Outer Space Treaty (1967) is at the heart of space governance: it is the framework document for the exploration and use of space, guarantees its neutrality, as well as prohibits the deployment of weapons of mass destruction in orbit.[44] Crucially, it does not prohibit the placement of other weapons, the use of space to advance military objectives, or the broader militarisation of Earth's orbit. The wording of the treaty is sufficiently vague so as to allow ample leeway for states to interpret it to meet their own national priorities and needs.

One of the challenges to governance is that the use of space has evolved in the decades since the Outer Space Treaty was adopted, and there are now several areas where current arrangements are insufficient, particularly related to military operations in space. Attempts to address these deficiencies - such as the placement of weapon systems in space - are most visible in the proposed Prevention of an Arms Race in Space (PAROS) Treaty,[45] first introduced as a resolution at the UN General Assembly (UNGA) in 1981. As of January 2023, work continues on PAROS, now heavily promoted by Russia and China, but effectively vetoed by repeated 'no' votes of the US. In the years since its initial introduction, a number of other resolutions relating to the militarisation of space have been presented before the UNGA, and whilst resolutions are not legally binding, they are a good indication of national positioning on particular space issues. Since 2014 for example, a resolution that would seek to prevent the first placement of weapons in outer space has been placed annually before the UNGA: the US has consistently voted against the resolution, and between 2014 and 2017 all the remaining members of NATO abstained. Since 2018 an increasing number of NATO members have joined the US in opposing

the motion (seven in 2019, increasing to 22 in 2020 & 2021).[46] 2020 indicates a sea-change in Alliance members approaches to the issue, and in December 2022, twenty-eight of the thirty NATO members voted against the resolution (North Macedonia and Türkiye have no recorded vote). Voting records suggest that as of 2019 - in the wake of the formation of US Space Force, the inauguration of several national space commands, and the adoption of NATO's own space policy and its declaration of space as an 'operational domain' - the Alliance's attitude and approach to space governance became more coordinated. Its approach has become more entrenched in maintaining its ability and flexibility to act, and not to cede deployability: resisting attempts to establish rules and norms that would limit its strategic manoeuvrability and ability to act within space.

Whilst the UN continues to support work on the PAROS Treaty, it has also encouraged the pursuit of 'other measures' that could contribute to stability and security in space. Attempts to pursue such measures have proceeded in earnest - and often with enthusiastic NATO support. This was evident in 2020 with the adoption of a UK championed resolution relating to the reduction of threats in the domain through the adoption of accepted norms and rules.[47] This resolution was subsequently represented to and readopted in 2021.[48] Another measure that has commanded support are US-sponsored efforts to halt destructive DA-ASAT testing, with the UNGA adopting a resolution to that effect in December 2022.[49] Whilst the resolution does not require compliance, it does encourage nations to behave responsibly in the space environment, to ensure continued security and safety, and begin the process of establishing collaboratively developed rules and behaviours. Those countries voting against included China and Russia, and India who abstained:[50] three nations that have already successfully demonstrated DA-ASAT capability. Ironically China and Russia are also simultaneously proponents of limiting the ability of nations to deploy weapons in space, and of continued work on the *PAROS Treaty*.

These 'other measures' are not designed to promote arms control, prevent the deployment of military capabilities, or limit the ability to execute national security objectives in the space domain. In this light NATO's reluctance to support resolutions designed to control development or limit deployment are understandable: Johnson-Freese and David Burbach observe that whilst the principles underpinning these resolutions have often 'gained traction', they invariably fail to command continued support when dominant space powers felt that 'emerging norms would erode their edge'.[51] Efforts that do command broad support are those designed to reduce opportunities for miscalculation, lessen the likelihood of accidental engagement, contact or damage, and to constrain the possibility of escalation. It can be inferred from the Alliances actions within the UN that its members support the measures to increase stability - but they are only willing to do so on their terms. Terms that do not limit their tactical, operational, or strategic capabilities or diminish their present advantages in space, nor limit their ability to act in, from or through the domain. Governance is also an inherently political decision, and a nation's approach to these issues - particularly on the international stage - is reflective of their government's current approach to national security. This can be

visualised through the attitude of the US; the tone and approach of the US administration to collaborate in security and international norms is distinctly different from those expressed in its previous administration: who is to say what the next administration will prioritise in the area of space governance? Any progress made now could be short lived and generate increased uncertainty and instability in the medium to long term.

Whilst international governance and national policies are still in their nascency, and whilst NATO continues to encourage and enhance cooperation between members, it is clear that the defence of allied space infrastructure is envisaged to be undertaken at the collective level. This is not necessarily a credible strategic position: approaches are predicated on a collective interoperability in an arena where the alliance does not have a tested and available material capability with which to respond in the domain and has not yet formalised the mechanisms required for interoperability and deterrence in space at the tactical or operational levels. This is compounded by differing approaches towards operations in space, a governance structure that is severely limited by design - because of the collective political and diplomatic weight of the Alliance - and an unwillingness to surrender strategic advantage in the face of strategic competitors. Much like collective defence, international agreements and treaties are only effective if the majority agree to abide by, regulate and enforce its provisions and commitments: without the majority of major space powers - of which the US and a number of its allies constitute a considerable number - there can be no effective governance in an increasingly busy and challenging environment. Without appropriate governance, and a recognition and acceptance of sustainable rules, norms and behaviours, the likelihood of miscalculation or hostile events in the space domain continues to increase, and so too does the need for a robust response.

Collective Defence

Article V of the North Atlantic Treaty embodies the principle that an attack on one is an attack on all.[52] The key to collective defence however is not in Article V, but in Article VI, which stipulates the geographical conditions necessary to trigger Article V. Article VI specifies that eligible events are any attacks on 'the territory of any of the parties in Europe or North America… [and] of Turkey… [and any] islands under the jurisdiction of members in the North Atlantic area north of the Tropic of Cancer.'[53] The Article further extends this to include attacks on the forces, vessels, and aircraft of members when 'in or over these territories… or the Mediterranean Sea or North Atlantic area…'. There is no mention of the new global commons of cyberspace or space, or of digital infrastructure or satellites.

Designed for a Different Era

When the North Atlantic Treaty was drafted, neither cyber nor space were credible or realistic operating domains. Why then, has NATO has not taken steps to amend or update the Treaty in light of their emergence? It has done so previously to reflect the accession of new members: Article VI was amended in 1951 upon the accession of Greece and Turkey, and in 1962 to reflect the changing status of the former Algerian Departments of France.[54] It could be argued

that the delay in updating the Treaty represents a bold strategic move, designed to increase ambiguity and confusion over the limits and application of collective defence, and bolster the deterrence capability of the Alliance in the face of increasingly emboldened and provocative adversaries. Conversely, it could be that the extant and out-of-date wording is reflective of an organisation that is still trying to find its feet in a new and dynamic strategic operating environment: an Alliance that is trying to establish where its core function of collective defence sits within these new diffuse operating areas, and how the limitless boundaries of cyber and space apply within an organisation defined by its territorial limits. There is a third option: the idea that the principles of collective defence are so well understood, and have been so well articulated – even in the areas of cyber and space – that the wording of Articles V and VI, whilst undoubtably requiring an update to reflect the new operating environments, is not an immediate priority for the Alliance when compared to the increased operational workload that NATO and its members are already undertaking across multiple domains in response to emerging threats.

Whatever the reason, any update to the Treaty would need to be explicit: a clear statement of boundaries, thresholds and intent which defines the circumstances and conditions under which collective action could be taken in the new domains: does it include all NATO members' spaceborne assets, civilian and military? What happens if the target is a civilian asset, targeting by a military asset or vice versa? Who is responsible if a civilian asset is used to intentionally damage a civilian satellite with secondary-military use? Does it only apply to assets in particular orbits, or above specified altitudes? What of a cyber-attack on a civilian contractor supplying military satellite services? There is an opportunity for the Alliance to answer these questions and to update its legal framework with the impending accession of Finland and Sweden, but even if these questions were to be answered – and there is little evidence from NATO to suggest that they have been - exactly what any collective response might entail remains a topic of intense debate and ambiguity.

To Action: Article V

Action is derived from Article V, the article providing for collective defence. There is a perception that the article provides for unambiguous, military centric, collective defence. Invocation is itself a political decision and is not – as Rose Gott Moeller et al observe - an 'automatic escalation pathway',[55] and will not necessarily necessitate military action. The reality is that it calls for 'such action as it deems necessary, *including* [author emphasis] the use of armed force', and NATO's responses to date – including its post 9/11 response - are characterised by hybrid, innovative solutions designed to prevent escalation, and which do not always include the explicit *use* of force. This is demonstrated through a number of deployments intended to demonstrate resolve and enhance deterrence: including the deployment of the NATO Response Force in 2022 in response to Russian aggression towards Ukraine (a non-NATO member, but bordering member states).[56] The deployment represents a willingness to fight, a capability to fight with, and a force that can be used for military deterrence, but also in support of diplomatic efforts by virtue of its being. Is it possible for the

Alliance to achieve similar outcomes in the complex operating domain of space: to leverage political, economic, and diplomatic weight to preserve stability? Evidence suggests that these are the *only* realistic options available given the lack of offensive or defensive space capability. Whilst cyber is touted as a likely response, and its impact on infrastructure could be substantial, it remains – broadly - untested, and is by its very nature, diffuse: can a response be credible if its origins are ambiguous, and it is not seen to be deployed? For Article V to be a credible deterrent to events in *any* domain, the Alliance's policy must keep pace with the rapid advances in technology, and they must visibly possess the capability, and the collective will to act. Whilst it possesses these in the land, maritime and air domains, it does not in the areas of the new global commons, weakening the effectiveness of collective defence.

When NATO declared cyber an operational domain in 2014, it stated that a cyber or hybrid attack *could* be justification for Article V invocation: this was repeated when space was declared an operational domain in 2019, and reiterated in the *2022 Strategic Concept* whereupon 'a single or cumulative set of malicious cyber activities; or hostile operations to, from, or within space; *could* reach the level of armed attack … to invoke Article V …'.[57] Against what metric would such an invocation be made, and with what capability would the response be rendered? There are two criteria that must be fulfilled for collective deterrence to succeed: the ability to successfully identify and attribute an attack, and the availability and acknowledgement of a credible, appropriate response by both the defender and the aggressor.

Attribution

Bedford and Giarra note that 'as the commons grow more complex, securing them becomes more difficult'.[58] NATO must first establish if an attack has occurred. If an attack is identified, it must still be attributed to a perpetrator: where a missile is utilised it is likely that the launch will be detected at launch and in flight, making attribution more likely – but what if the damage is caused by another satellite, or via a cyber-attack against satellite ground stations? The number of satellites and debris in orbit mean that damage could be caused by accident rather than aggression. What if a nation deliberately targets its *own* satellites to generate debris that subsequently damages an allied satellite – an 'accidently-on-purpose' event? NATO is accustomed to a geographically focussed defence posture where threats originate under predictable, detectable, and observable conditions. The nature of the new global commons makes this increasingly difficult: attacks may be multi-faceted, diffuse, and not easily attributable.

Establishing whether an attack has occurred is complicated further by the increased involvement of the commercial sector in space capability provision. Commercial partnerships have long been associated with the defence industry, but the lines between military and civilian capability are now more blurred than ever, particularly so in space. National governments are increasingly reliant on commercial companies, such as Airbus and Space X, for a range of space functions including SATCOM, space launch services, logistics

services and SDA provision. NATO's own SATCOM provision is provided by a collaborative partnership which utilises the capabilities of some of its members, including France and the UK: both the UK's *Skynet* military satellite system, and the ground operating segments of the French *Syracuse* system are operated by Airbus.[59] Many of these partnerships have also resulted in 'dual-use' satellites: civilian satellites where bandwidth and capacity are leased to militaries and governments.[60] Dual-use satellites introduce a further variable into the strategic calculus: what if a commercially owned satellite is engaged by an aggressor? Does this constitute an armed attack against the territory of a state, or one of its emanations? A satellite is not the same as a ship, aircraft, or embassy. What if the company is headquartered and registered in another country - has that country been attacked also? What if the company leases services on the same platform to multiple nations: have they all been attacked? Does an attack on a dual-use satellite also providing civilian communications function constitute an attack on civilian infrastructure? These questions have no simple answer, but the increased commercialisation of space and the reliance on which militaries now place on these arrangements mean that ownership and the role of assets is often blurred: each dual-use satellite in orbit represents a possible aggressor, a possible target, and a possible pandora's box of legal uncertainty and strategic ambiguity.

It is fortunate - given the complexity of the operating environment, the range of threats, and the challenge of attribution - that NATO has a robust mechanism for considering its invocation of collective defence, and for employing the use of force. Whilst Article V itself does not constitute an escalation pathway, the North Atlantic Treaty provides for a series of steps designed to allow for investigation, verification, attribution, discussion and - when required - response. It provides for an individual nation to call together the other members for consultation in the event that they believe their security has been threatened - a precursor to subsequent action.[61] This process was recently exercised informally, and in full public view, in November 2022 when a missile - initially suggested to have been fired by Russia during the course of operations in Ukraine - veered off course and landed in Poland, resulting in the deaths of two civilians. Amidst intense media scrutiny, speculation, uncertainty, and increasing calls to respond, NATO *was* quick to act not to respond materially under Article V, but instead to utilise its shared resource, capabilities and experience to establish the facts.[62] The conclusion - reached relatively quickly - was that the missile was in fact a wayward Ukrainian missile that had been engaged against Russian missiles, and that the event - whilst unfortunate - was an accident. This case aims to illustrate the inherent strength of NATO, but also a fundamental flaw when dealing with the new global commons: the system is designed to function, and functions best, when the threat area is defined by geographical boundaries and the threat origin can be ascertained and proven. Had an incident, similar in nature to that of November 2022 occurred in the space domain, would the response have been the same? Space is global, without territorial limit, and the threat is diffuse. Would NATO have had the capability to attribute an attack, to differentiate between accidental and on-purpose? And, perhaps crucially, would it have the capability to respond, if it was decided that an attack had occurred, and Article V invocation was appropriate?

A Requirement for a Credible Response

Militarily, collective defence is embodied by conventional forces that have a proven record of operating together and characterised by a willingness to utilise them. Within NATO, this defence is underwritten by the independent nuclear arsenals of the US, UK, and France – the ultimate deterrent, designed to counter the capabilities of Russia, and increasingly, China. These forces routinely operate across the land, maritime and air domains, and their capabilities are recognisable – carrier strike and amphibious task groups deployed simultaneously to the High North and the Mediterranean, multi-national battlegroups deployed to Eastern Europe, and allied air forces conducting regular interdiction and escort duties across the entire length and breadth of allied territory. An incursion into NATO airspace by an adversary's aircraft is met by armed interdiction aircraft, and any foray by land forces into Alliance territory will invoke the full force of a NATO battlegroup. We know this because it has been articulated by officials, exercised extensively, and in many cases, executed operationally. NATO's commitment to security across the land, maritime and air domains is visible and recognisable. No comparable response exists with respect to space.

NATO's adversaries have a wide arsenal of credible offensive weapons that are tested, operational, and available: the means to directly defend against kinetic strikes targeting orbital assets are not, save an offensive response against an aggressor's own assets or ground stations. Even this would be subject to a national veto, and the only Alliance member with potential kinetic counter-space technology is the US, though this is based on adapted technology and not readily available for deployment. There is also recognition that the use of kinetic counter-space weaponry will add to the risks posed by debris – defending states may be reluctant to further risk their space infrastructure, lest they inadvertently exacerbate their losses, or inflict damage on or cause the loss of allied assets. Responses to any attack will invariably be undertaken by the traditional conventional forces of the alliance upon earthbound infrastructure, or via cyber-attack: though cyber offensive capability remains a closely guarded secret and is arguably still in development and lacking operational maturity. Furthermore, operational cyber-response has not yet been *seen* to be deployed by NATO, diminishing its deterrence effect.

A Grand Design or Accidental Convenience?

The space domain has generated the perfect storm of challenges for NATO. Discrete areas – attitudes towards militarisation and governance, and a reluctance to surrender strategic advantage, inconsistency in national approaches, and uncertainty surrounding the reach and application of collective defence - create an ambiguity upon which it is difficult for adversaries to assess the outcome of any action against the Alliance. The US has been unequivocal in its policy to respond to any attack or interference in space, despite its inexperience in waging war in the environment: now with a change of administration it is less equivocal and has pivoted more towards the creation of norms and international standards. It remains, however, the preeminent space-faring nation, with a verified ability to deploy offensive weaponry on a global *and* orbital scale. The issue becomes opaquer when considering the other twenty-nine

members of NATO: without sovereign offensive capabilities they are beholden to the Alliance – to the US - for a credible and robust kinetic response in space. Liselotte Odgaard observes that, despite asymmetry in balance of forces and capability, the Alliance must ensure a joint response to the Chinese and Russian threats:[63] as policy and capability presently exist, this is not the case. This creates an 'unknown' in planning, and the lack of recognised thresholds for Article V invocation in the space and cyber domains further complicate the strategic mathematics: the uncertainty as to what constitutes an attack. Such thresholds undoubtably do exist, but by concealing this information NATO arguably bolster its defensive posture, though Gott Moeller et al note that withholding threshold knowledge from adversaries could embolden them to act.[64] The question is whether deterrence in the space domain operates according to the same rules as in the traditional domains, and whether opponents believe that it does.[65] Indeed, proponents within NATO argued in 2020 that the Alliance should 'consider making its Space Policy adequately available to the public', as it does with other major policies for other domains.[66] In doing so NATO would remove some of the ambiguity that permeates its approach to space, and would reassure allies and interested parties that there were answers to the ever-increasing array of questions. Or, at the very least, provide assurance that steps were in place to address the seemingly large deficits that the domain has generated in the Alliances collective defence posture. Concurrently, it would serve as a warning to potential opponents: we have the answers, we have a plan, and we are ready.

Nevertheless, NATO's space policy remains a closely held secret. Regardless of whether this is a policy of deliberate ambiguity or not, it serves as a powerful strategic multiplier that takes advantage of a state's inherent aversion to risk, ultimately increasing the deterrence effect. NATO has 'vowed to clarify' its collective defence commitments with respect to space and cyber,[67] but until it does so, ambiguity will remain.

Conclusion

As more nations look to the stars for advantage, and as the planet's orbits become increasingly congested, space security will only grow in complexity. It would be convenient to be able to say that 'the space domain is, without a doubt, an '"x" domain', but the reality is that it is simultaneously a warfighting, operational and ambiguous domain: a tinderbox of emergent capability, nascent and underdeveloped governance, and divergent national approaches. No-one questions the strategic importance of securing space, but analysis is based on limited information, conjecture, speculation, and an application of doctrine designed for the domains of land, sea, and air. The renewed 'space race' is characterised by voluminous policy documents, vague declarations of ambition, statements of intent, and press releases. It will take an incident in the domain for thresholds and responses to be fully tested, and for their effectiveness to be assessed. Fortunately, for the time being, offensive interactions in space have been limited to capability tests by a limited roster of nations.

We find ourselves in an environment where the speed of technological advancement outstrips our ability to legislate, our ability to control and mitigate, and our ability to generate

appropriate frameworks and strategies to respond and react to threats in good time. Despite best efforts, NATO's collective approach to operations and security in space is reactive rather than visionary. As threats continue to evolve, it is an unfortunate truth that NATO appears to have attempted to make policies and initiatives 'fit' inside its existing security architecture: an architecture that is not necessarily robust or flexible enough for a twenty-first century battlespace that encompasses the entirety of the planet, simultaneously and perpetually. NATO may only be able to operate – for the foreseeable future - *through* space, rather than *in* space - to support operations, rather than command and occupy the domain. A schism exists within NATO insofar that the US continues to eschew international limitations on its capabilities and strives for political and material supremacy in the domain, and to secure its 'edge'. This contrasts with the remainder of the Alliance where they are content to secure space as an enabling domain and focus their resources and policy thus, relying on the principle of collective defence and deterrence to mitigate against adversarial advancements.

Nevertheless, opponents face uncertainty should they engage NATO in the space domain: the capabilities to respond do exist, and the potential cost to the aggressor - if attributed - could be substantial. The exact nature of any response remains ambiguous, whether by design or accident, ultimately lending credibility to the idea of collective defence, and enhancing the deterrence posture that is at the heart of the Alliance. Despite this ambiguity that permeates NATO's space posture, members commitments to protecting their space infrastructures is unambiguous, and the fact remains that in times of crisis, NATO displays an unyielding and unparalleled capacity for cooperation and decisive action across all aspects of warfare: political, economic, diplomatic and – when required – militarily. Member states must hope that a response to an incident in the space domain is no different.

Notes

[1] French Ministry for the Armed Forces. 'Space Defence Strategy', (Paris, 2019); UK MOD, 'Defence Space Strategy: Operationalising The Space Domain' (London: HMSO, 2022).
[2] Victor Mallet, 'France follows US to set up military space command', *Financial Times*, 14 July 2019, www.ft.com/content/a479bcb6-a628-11e9-984c-fac8325aaa04, accessed 23 September 2022; Sabine Siebold, 'New German Space Command To Tackle Russian, Chinese Threat, Overcrowding', *Reuters*, 13 July 2021, www.reuters.com/business/aerospace-defense/new-german-space-command-tackle-russian-chinese-threat-overcrowding-2021-07-13, accessed 23 September 2022; UK Government. 'UK Space Command Officially Launched', 30 July 2021, www.gov.uk/government/news/uk-space-command-officially-launched, accessed 22 September 2022.
[3] UK Ministry of Defence (MOD), 'Joint Concept Note 1/20 Multi Domain Integration' (London, 2020), p. 74.
[4] NATO, 'NATO 2022 Strategic Concept', 29 June 2022, (Brussels, 2022), p. 6-11
The Alliance identifies a number of core themes as its core tasks: *Deterrence and Defence, Crisis Prevention and Management,* and *Cooperative Security*, with the ability to deter, defend, contest, and deny across all domains and in all directions.

[5] Thierry Tardy, 'The risks of NATO's maladaptation', *European Security*, Vol. 30, No. 1 (July 2020) p. 26.
[6] Thierry Tardy, 'The risks of NATO's maladaptation', p. 27.
[7] Evanthis Hatzivassiliou, 'The View From NATO: Sputnik As A Catalyst, 1957–8', The International History Review Vol. 42, No. 6 (2019), p. 1137-1138.
[8] NATO, 'NATO 2022 Strategic Concept' p. 5.
[9] US DIA, 'Challenges To Security In Space: Space Reliance In An Era Of Competition And Expansion', 2022, p. 3-4.
[10] US DIA, 'Challenges To Security In Space: Space Reliance In An Era Of Competition And Expansion', p.iii.
[11] William J. Broad & David E. Sanger. 'China Tests Anti-Satellite Weapon, Unnerving U.S', *The New York Times*, 18 Jan 2007, www.nytimes.com/2007/01/18/world/asia/18cnd-china.html, accessed 23 September 2022; Government of India, 'Frequently Asked Questions on Mission Shakti, India's Anti-Satellite Missile test conducted on 27 March 2019', 27 Mar 2019, www.mea.gov.in/press-releases.htm?dtl/31179/Frequently_Asked_Questions_on_Mission_Shakti_Indias_AntiSatellite_Missile_test_conducted_on_27_March_2019, accessed 30 September 2022; NATO, 'Statement by the North Atlantic Council on the recent anti-satellite missile test conducted by the Russian Federation', Press Release (2021) 170, 19 Nov 2021, www.nato.int/cps/en/natohq/news_188780.htm, accessed 27 October 22.
[12] Joan Johnson-Freese & David Burbach, 'The Outer Space Treaty and the Weaponization of Space', *Bulletin of the Atomic Scientists* Vol. 75, No. 4 (2019), p. 137-138.
[13] Garcia, Mark, 'Space Debris And Human Spacecraft', NASA, 2022, www.nasa.gov/mission_pages/station/news/orbital_debris.html, accessed 30 September 2022.
[14] Black, Samuel & Butt, Yousaf, 'The Growing Threat of Space Debris', *Bulletin of the Atomic Scientists* Vol. 66, No. 2 (2010), p. 2.
[15] Jürgen Scheffran, 'Dual-Use in a New Security Environment - The Case of Missiles and Space', *INESAP Information Bulletin*, No. 26, (June 2006), p. 50.
[16] UK Government. 'United Kingdom National Submission on Space Threats to respond to the call from UN Secretary General under the UN GA Resolution A/RES/75/36 on Reducing Space Threats through norms, rules and principles of Responsible Behaviour', 30 April 2021, https://front.un-arm.org/wp-content/uploads/2021/05/national-submission-of-the-United-Kingdom-in-connection-with-resolution-75_36.pdf, accessed 22 December 2022, p.8.
[17] Benjamin Staats, 'Mitigating Security Risks and Potential Threats of Emerging Rendezvous and Proximity Operations', *Astropolitics* Vol. 20, No. 1 (2022), p. 67.
[18] AFP, 'Russia Rejects Space Weapon Claim as 'Propaganda'', *The Moscow Times*, 24 July 2020, www.themoscowtimes.com/2020/07/24/russia-rejects-space-weapon-claim-as-propaganda-a70964, accessed 29 September 2022.
[19] Kamala Harris, 'Remarks by Vice President Harris on the Ongoing Work to Establish Norms in Space', 18 April 2022, Transcript, www.whitehouse.gov/briefing-room/speeches-remarks/2022/04/18/remarks-by-vice-president-harris-on-the-ongoing-work-to-establish-norms-in-space, accessed, accessed 25 October 2022.

[20] Benjamin Rojek, 'JSpOC integral to Burnt Frost success,' US Space Force - Vandenberg Space Force Base, 29 February 2008, www.vandenberg.spaceforce.mil/News/Article-Display/Article/340906/jspoc-intergral-to-burnt-frost-success, accessed 2 December 2022.
[21] United Nations, *Legal Subcommittee of the Committee on the Peaceful Use of Outer Space*, 767th meeting, UN Document COPUOS/LEGAL/T.767, 1 April 2008, www.unoosa.org/pdf/transcripts/legal/LEGAL_T767E.pdf, accessed 12 November 2022, p. 19.
[22] Germany Federal Foreign Office, 'Germany commits in Geneva not to conduct anti-satellite direct-ascent missile tests', 13 September 2022, https://www.auswaertiges-amt.de/en/aussenpolitik/themen/anti-satellite-missile-tests/2551852, accessed 14 December 2022; UK Government, 'Responsible space behaviours: the UK commits not to destructively test direct ascent anti-satellite missiles', 3 October 2022, www.gov.uk/government/news/responsible-space-behaviours-the-uk-commits-not-to-destructively-test-direct-ascent-anti-satellite-missiles, accessed 4 October 2022; French Ministry for Europe and Foreign Affairs, 'Space - France's commitment not to conduct destructive direct-ascent anti-satellite missile tests', 29 November 2022, www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/2022/article/space-france-s-commitment-not-to-conduct-destructive-direct-ascent-anti, accessed 14 December 2022; Canadian Government, Twitter Post, 9 May 2022, 4:25 pm, https://twitter.com/CanadaGeneva/status/1523685496399966209.
[23] NATO, 'NATO 2022 Strategic Concept', p. 5.
[24] US Government, 'National Security Strategy'. (Washington DC, October 2022), p. 11
[25] Pierre Haroche & Martin Quencez, 'NATO Facing China: Responses and Adaptations', *Survival*, Vol. 64, No. 3 (June – July 2022) p. 74-75.
[26] Pierre Haroche & Martin Quencez, 'NATO Facing China: Responses and Adaptations', p. 80
[27] Everett Dolman, 'Space is a Warfighting Domain', *Æther Journal of Strategic Airpower & Spacepower*, Vol. 1, No. 1 (Spring 2022), p. 87.
[28] UK Ministry of Defence (MOD), 'Joint Concept Note 1/20 Multi Domain Integration' (London, 2020), p. 21
[29] Everett Dolman, 'Space is a Warfighting Domain', p. 88.
[30] Everett Dolman, 'Space is a Warfighting Domain', p. 85.
[31] Donald J Trump, 'Remarks By President Trump At Signing Ceremony For S.1790, National Defense Authorization Act For Fiscal Year 2020', 20 December 2019, Transcript https://trumpwhitehouse.archives.gov/briefings-statements/remarks-president-trump-signing-ceremony-s-1790-national-defense-authorization-act-fiscal-year-2020, accessed, 2 October 2022.
[32] Steve Lambakis, 'Space As A Warfighting Domain: Reshaping Policy To Execute 21st Century Spacepower', *Comparative Strategy* 41, No. 4 (2022), accessed 27 September 2022, p. 332.
[33] US Government, 'National Security Strategy of The United States of America'. (Washington DC, Dec 2017), p. 31.
[34] US DoD, 'Defense Space Strategy Summary' (Washington DC, June 2020), p. 2.
[35] US DoD, 'Defense Space Strategy Summary', p. 7.
[36] US Government, 'National Security Strategy', p. 45.

[37] NATO, 'London Declaration', 4 Dec 2019, www.nato.int/cps/en/natohq/official_texts_171584.htm, accessed 29 September 2022.
[38] NATO, 'NATO's overarching Space Policy', 17 Jan 2022, www.nato.int/cps/en/natohq/official_texts_190862.htm, accessed 1 October 2022.
[39] NATO, 'NATO's overarching Space Policy'.
[40] French Ministry for the Armed Forces, 'Space Defence Strategy', 2019, p. 36.
[41] French Ministry for the Armed Forces, 'Space Defence Strategy', 2019, p. 26.
[42] Dominic Vogel, 'German Armed Forces Approaching Outer Space: The Air and Space Operations Centre As a Gateway to Multi-Domain Operations', SWP Comment (Berlin: German Institute for International and Security Affairs, October 2020), p. 2.
[43] UK MOD, 'Defence Space Strategy: Operationalising The Space Domain', p. 30-32.
[44] 'Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies', opened for signature on 27 January 1967, entered into force on 10 October 1967, 610 UNTS 205, https://treaties.un.org/doc/Publication/UNTS/Volume%20610/v610.pdf, accessed 31 October 2022.
[45] United Nations General Assembly, 1981. *Resolution adopted by the General Assembly on 9 December 1981 - Prevention of an arms race in outer space*. Thirty-sixth session. A/RES/36/97 C. Available at https://digitallibrary.un.org/record/610780, accessed 16 December 2022.
[46] Based on analysis of results for UN General Assembly votes on the resolution entitled 'No first placement of weapons in outer space' between 2014 and 2022, obtained from the *United Nations Digital Library Voting Data Collection* at https://digitallibrary.un.org. Links to individual voting record pages are contained in the Reference List.
[47] United Nations General Assembly, 2020. *Resolution adopted by the General Assembly on 7 December 2020 - Reducing space threats through norms, rules and principles of responsible behaviours*. Seventy-fifth session. A/RES/75/36. Available at https://digitallibrary.un.org/record/3895440, accessed 3 December 2022.
[48] United Nations. 'Reducing space threats through norms, rules and principles of responsible behaviours' *United Nations Digital Library [Voting Data Collection]*, 24 December 2021, https://digitallibrary.un.org/record/3952170, accessed 12 November 2022.
[49] United Nations General Assembly, 2022. *Resolution adopted by the General Assembly on 7 December 2022 - Destructive direct-ascent anti-satellite missile testing*. Seventy-seventh session. A/RES/77/41. Available at https://digitallibrary.un.org/record/3997622, accessed 3 January 2023.
[50] United Nations, 'Destructive direct-ascent anti-satellite missile testing', *United Nations Digital Library [Voting Data Collection]*, 7 December 2022, https://digitallibrary.un.org/record/3996915, accessed 21 December 2022.
[51] Joan Johnson-Freese & David Burbach, 'The Outer Space Treaty and the Weaponization of Space', p. 139.
[52] NATO, 'Collective defence and Article 5', 20 Sep 2022, www.nato.int/cps/en/natohq/topics_110496.htm, accessed 30 September 2022.
[53] 'North Atlantic Treaty' 4 April 1949. www.nato.int/cps/en/natolive/official_texts_17120.htm, accessed 1 October 2022.

[54] 'Protocol to the North Atlantic Treaty on the Accession of Greece and Turkey' 22 October 1951, www.nato.int/cps/en/natohq/official_texts_17245.htm, accessed 21 October 2022.
[55] Rose Gottemoeller et al., 'Engaging With Emerged And Emerging Domains: Cyber, Space, And Technology In The 2022 NATO Strategic Concept', *Defence Studies* 22, no. 3 (2022), p.519.
[56] NATO, 'NATO Response Force', 11 July 2022, www.nato.int/cps/en/natolive/topics_49755.htm, accessed 3 October 2022.
[57] NATO, 'NATO 2022 Strategic Concept', p. 7.
[58] Dick Bedford & Paul Giarra, 'Securing the Global Commons', *The RUSI Journal*, 153(5) (2010), p. 21.
[59] Airbus. 'Skynet 5', www.airbus.com/en/products-services/defence/milsatcom/skynet-5, accessed 19 November 2022; Airbus. 'Airbus wins the first Syracuse IV ground segment programme contract', Press Release, 4 March 2021, www.airbus.com/en/products-services/defence/milsatcom/skynet-5, accessed 19 November 2022.
[60] Sarah Casenove. 'Commercial Satellite Communications in the Military domain', *Airbus*, https://securecommunications.airbus.com/en/meet-the-experts/commercial-satellite-communications-in-the-military-domain, accessed 19 November 2022; Erwin, Sandra. 'SpaceLink partners with Parsons for DARPA's inter-satellite communications project,' *Space News*, 22 August 2022, https://spacenews.com/spacelink-partners-with-parsons-for-darpas-inter-satellite-communications-project, accessed 19 November 2022.
[61] 'North Atlantic Treaty', Article IV.
[62] NATO, 'NATO Allies address the explosion in the east of Poland', News Release, 16 November 2022, www.nato.int/cps/en/natohq/news_209104.htm, accessed 3 December 2022.
[63] Liselotte Odgaard, 'NATO's China Role: Defending Cyber and Outer Space', *The Washington Quarterly*, Vol. 45, No. 1 (2022), p. 174.
[64] Rose Gottemoeller et al., 'Engaging With Emerged And Emerging Domains: Cyber, Space, And Technology In The 2022 NATO Strategic Concept', p. 518.
[65] Rose Gottemoeller et al., 'Engaging With Emerged And Emerging Domains: Cyber, Space, And Technology In The 2022 NATO Strategic Concept', p. 518-519.
[66] NATO Reflection Group, 'NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General', 25 November 2020, www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf, accessed 3 November 2022, p. 47.
[67] Liselotte Odgaard 'NATO's China Role: Defending Cyber and Outer Space', p. 175.