North Atlantic Treaty Organization and Space:

Recommendations for a New Space Policy

Emilyn Tuomala, Kyle O'Keefe, Jacob Baker[1]

The George Washington University
Elliott School of International Affairs

[1] The views expressed here are the authors' personal views and should not be attributed to LLNL or its sponsors.

This work was performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344. LLNL-MI-830526

TABLE OF CONTENTS

I. Executive Summary

The space domain is undeniably vital to human existence and security. Recent operations conducted by the United States and other actors demonstrate the growing efficacy of space systems and point to their increasing importance in global security dynamics. Despite the centrality of space-based capabilities to diplomatic, informational, military, and economic power, challenges continue to plague policymakers in determining the optimal approach to acquiring, employing, and organizing space-based capabilities, specifically in the context of a key multilateral security organization—the North Atlantic Treaty Organization (NATO).

NATO has fundamentally altered its approach to the space domain over the past three years. While NATO's history in space dates back to the beginning of the Cold War, it is only now that NATO is incorporating space into its general posture instead of predominately relying on its use for communications. In 2018, Allied leaders at the Brussels Summit recognized space as a "highly dynamic and rapidly evolving area" and proceeded to codify NATO's first space policy in a classified document in 2019. Following the codification, space was declared a new operational domain in the same manner as land, sea, air, and cyberspace. Furthermore, NATO established a new Space Center at Allied Air Command in October of 2020. However, uncertainty still exists around how NATO would respond to an attack on member countries' space assets and what collective defense means within the context of the space domain.

To rapidly advance the dialogue on and evolution of NATO space policy, this paper analyzes appropriate concepts, methods, and insights from the cyber domain and NATO's strategic capabilities concept to determine their applicability for a new NATO space policy. As such, this paper also seeks to answer important questions including, but not limited to, the following: Should NATO fund the development of its own space capabilities? Will future space conflict warrant a natural continuation of NATO deterrence policy, or should clearer thresholds be drawn? What challenges exist with regards to the asymmetry of member space capabilities?

Ultimately, this paper yields four policy recommendations for NATO to consider. NATO's main mission must be to ensure its deterrent capability and the strength of its alliance while incorporating the increasingly vital space domain. In order to achieve this, NATO must codify its flexibility in response as part of future space policies. Additionally, NATO should establish a Space Planning Committee to guide its efforts in the domain, while simultaneously expanding its partnership with international entities and the private sector. Lastly, NATO should rely on its Centers of Excellence to drive policy and interoperability innovation. The incorporation of these policy recommendations will allow NATO to advance its current strategy of interoperability and information sharing to enable and enhance military operations in the air, land, sea, and cyber domains while providing flexibility to rapidly adapt its policy given the anticipated pace of change to the space domain in the near- to mid-term.

II. Methodology

To conduct this research, we adopted a combined method of process tracing and expert interviews. We first identified key concepts, actions, and trends relevant to the conversation of NATO space policy to compile a literature review for our own understanding. We thoroughly analyzed existing postures, open-source intelligence reports, and data pertaining to NATO member countries' advancements in space. We ultimately decided to pursue a comparative model approach and identify key similarities and differences between NATO's current approach towards space, its policy building of the cyber domain, and NATO's position on nuclear deterrence and strategic capabilities, as well as trace the considerations and issues leading to the development and implementation of these actions.

After completing this initial analysis, we conducted five interviews with current/former NATO officials, military leaders, and industry experts (*See Appendix A)*. Our statement of purpose, background of the topic, and proposed questions were provided to the interviewees beforehand. We then compiled our findings and results of these conversations into a matrix to cross-reference and compare the responses in order to identify commonalities, potential trends, and discrepancies. We categorized and assessed these findings against the strategic capabilities and cyber models to help guide our creation of recommendations.

III. Background and Challenges

Through its establishment of the new Space Center, release of a classified space policy, and the declaration of space as an operational domain all within the last three years, NATO has formally recognized the importance of space on its current and future operations. It is critically dependent on space to enable operations across all other operational domains. Yet, as attested to by NATO's Secretary General Jens Stoltenberg, the space policy is only a framework and needs to be filled with content as NATO's understanding of its role in space evolves.[2] But with the ever-growing exploitation of space by allies, strategic partners, commercial providers, and adversaries, NATO does not have the luxury of time to allow its space policy and posture to mature slowly. Furthermore, hostile actors are seeking to rapidly expand advanced counterspace capabilities. In February 2020, Russian satellites displayed "disturbing" behavior by stalking a United States spy satellite, creating a "potentially dangerous situation in space."[3] In April 2020, the Islamic Revolutionary Guard Corps (IRGC) launched Iran's first military space program satellite.[4] China

---

[2] Bradley Bowman and Andrew Gabel, "NATO Declares Space 'Operational Domain,' but More Work Remains," Defense News (Defense News, December 13, 2019), https://www.defensenews.com/opinion/commentary/2019/12/16/nato-declares-space-operational-domain-but-more-work-remains/.

[3] W.J. Hennigan, "Strange Russian Spacecraft Shadowing U.S. Spy Satellite, General Says." *Time Magazine*, February 20, 2020. https://time.com/5779315/russian-spacecraft-spy-satellite-space-force/.

[4] Mike Wall, "Iran Launches Its 1st Military Satellite into Orbit: Reports," Space.com (Space, April 22, 2020), https://www.space.com/iran-launches-first-military-satellite.html.

already has operational ground-based missiles that can hit satellites in low Earth orbit (LOE) with suspicion it will pursue such capabilities for additional orbital layers.[5] Such events highlight the threats faced by NATO member countries in, to, and from space and could find NATO in a position deliberating collective defense without a robust space policy to inform response options.

Evolution of Space as a Warfighting Domain

The foundation of the current contested, congested, and competitive nature of the space domain was laid during the Cold War. As tensions between the Soviet Union and the United States escalated following the end of WWII, space represented a new opportunity to prove technological superiority and extend military capabilities. The launch of Sputnik 1 in October 1957 marked the start of a period of rapid Soviet technological advancements in satellites, rockets, and human space flight.[6] The United States and the Soviet Union accounted for 93 percent of all satellite launches during that period, of which 70 percent were military satellites.[7] The reliance on satellites to enable terrestrial military capabilities naturally led to the development of counterspace weapons. Early United States efforts in anti-satellite (ASAT) weaponry include Bold Orion in 1959 and Starfish Prime.[8] Meanwhile, the Soviet Union developed dedicated ASAT systems and leveraged residual capabilities meant for other purposes like ballistic missile defense. Development and testing of new space capabilities, to include ASAT weapons, extended well into the 1980s. The United States demonstrated its resolve too by its pursuit of the Strategic Defense Initiative (SDI) and the Air Launched Miniature Vehicle (ALMV).[9]

The result of technological advancements, rapid capability development, and a shared understanding of the harm deploying and using space weapons would have on both parties during the Cold War led to formal treaties and informal norms that continue to influence current space operations. The Partial Test Ban Treaty (PTBT), the Outer Space Treaty, the Anti-Ballistic Missile (ABM) Treaty, and SALT I created the legacy of cooperation and restraint that deters direct

---

[5] Defense Intelligence Agency. "Challenges to Security in Space," DIA, January 2019. https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

[6] James Clay Moltz, "*The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*," 82–123. Stanford, CA: Stanford University Press, 2019.

[7] Todd Harrison, Zack Cooper, Kaitlyn Johnson, and Thomas G. Roberts. "Escalation and Deterrence in the Second Space Age." Center for Strategic and International Studies, October 2017. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/171109_Harrison_EscalationDeterrenceSecondSpaceAge.pdf?pkaq8A3h5rRj8zkOrL2bDpUa4MtjERPa.

[8] Moltz, "*The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*," 155.

[9] U.S. Department of State. *Strategic Deterrence Initiative*, January 2009. https://2001-2009.state.gov/r/pa/ho/time/rd/104253.htm.

military confrontation and helps keep space free from orbiting weapons.[10] Following the ALMV tests in 1985, an informal moratorium agreed to by the Soviets and the United States on debris-producing testing in space advanced an international norm that was upheld until the Chinese launched an ASAT test in 2007.[11] The Cold War in space offered moments of cautious cooperation, open hostilities, and a shared understanding of the complexities of the domain.

With the fall of the Soviet Union and technological advancements proliferating to a broad range of state and non-state actors, the space domain became increasingly diverse. From 1991 to 2014, 43 percent of new satellites and 39 percent of launches were from nations other than the United States and Russia.[12] The increased number of assets in space from this range of actors highlighted the growing vulnerabilities of space capabilities. Much like in other domains, China pursued dual-use space systems and missile defense technology in LOE.[13] By 2007, Russia had begun modernizing its space and military capabilities for the first time since 1991.[14] This led to a period of space nationalism that inhibited the effective wholesale expansion of international norms. Despite attempts to engage in collective norm building in space, enduring national security concerns precluded any significant progress from being made toward specific stability-enhancing measures. Most notably, these failed attempts include the United States' decision to vote against the Prevention of an Arms Race in Space (PAROS) resolution in 2005—a treaty that had been unanimously approved every year since 1983—and the on-going tensions arising from the Sino-Russian proposed Prevention of the Placement of Weapons in Outer Space (PPWT), which Western governments oppose as it fails to address ground-based ASAT systems.[15]

The lack of international agreement on norms and behaviors in space presents a current environment that is more dangerous, diverse, and disordered then at any other point in history. More than 500,000 pieces of space debris indiscriminately threaten satellites and spacecraft.[16] Nations are developing increasingly sophisticated ASAT weapons to disrupt and disable satellites. Counterspace technology is commercially available to state and non-state actors. While greater scientific knowledge surrounding space environmental risks continues to favor national restraint

---

[10] Moltz, "*The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*," 155.

[11] Carin Zissis, "China's Anti-Satellite Test." Council on Foreign Relations, February 2010. https://www.cfr.org/backgrounder/chinas-anti-satellite-test.

[12] Todd Harrison, Zack Cooper, Kaitlyn Johnson, and Thomas G. Roberts. "Escalation and Deterrence in the Second Space Age." Center for Strategic and International Studies, October 2017.

[13] Helena Legendra, "China's Pursuit of Advanced Dual-Use Technologies." IISS, December 18, 2018. https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance.

[14] "An Introduction to Russia's Military Modernisation." IISS, September 2020. https://www.iiss.org/blogs/analysis/2020/09/rmm-introduction.

[15] Moltz, "*The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*," 282, 310.

[16] Mark Garcia, "Space Debris and Human Spacecraft." NASA. NASA, April 14, 2015. https://www.nasa.gov/mission_pages/station/news/orbital_debris.html.

over direct military competition in space, the international community has not been able to agree on the necessary steps to drastically reduce the threat posed to state actors to, from, and in space.

Background on NATO Space Posture

Space is not a new frontier for NATO. In close coordination with the United States, NATO took its first step to leveraging the advantages of space by investing in two ground terminals to communicate with a United States satellite in 1967. This effort would eventually expand, with over 20 ground communication terminals deployed at the height of the Cold War hosted in 12 countries.[17] In the same year, NATO launched a communications satellite (SATCOM) program to develop two planned military communications satellites. On March 20, 1970, NATO 1 was launched from Cape Canaveral aboard a NASA launch vehicle.[18] By May 1970, NATO 1 was turned over to the Supreme Headquarters Allied Forces Europe. And in February 1971, NATO 2 was launched from Cape Canaveral.[19] NATO's satellite development program consisted of eight total satellites launched successfully into orbit, the final two of which were launched in the early 1990s. The SATCOM project allowed for safe and secure military communications until its decommissioning in the early 2000s. With the purposeful decommissioning of the SATCOM program NATO decided to rely, and continues to do so, on capabilities developed and owned by member states instead of its own satellites.

With technological advancements and the growing reliance on space-based capabilities throughout the first decade of the 2000s, NATO recognized that its posture toward space needed to evolve. In 2012, NATO established a Bi-Strategic Command Space Working Group. The purpose of the group was to develop direction and guidance for space support to NATO operations and recommending requirements across the Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DoTMLPF-P) spectrum to improve space support to NATO operations. The Bi-Strategic Command Space Working Group served as a foundation for the developments of NATO space operations in the late 2010s. Allied leaders at the Brussels Summit in 2018 recognized space as a "highly dynamic and rapidly evolving area" and decided to develop an overarching NATO space policy separate from the air domain.[20] The first official, classified NATO space policy was implemented in 2019, which serves as a framework for the alliance to "fill with content and different activities."[21] The final, major developments in the

[17] NATO, "NATO, We Have Lift off!" NATO. https://www.nato.int/cps/us/natohq/declassified_138278.htm.

[18] NATO 1, 2017. http://www.astronautix.com/n/nato1.html.

[19] *Ibid.*

[20] NATO, "Approche De L'OTAN Concernant L'espace." NATO, October 9, 2020. https://www.nato.int/cps/fr/natohq/topics_175419.htm?selectedLocale=en.

[21] Bowman and Gabel, "NATO Declares Space 'Operational Domain,' but More Work Remains," https://www.defensenews.com/opinion/commentary/2019/12/16/nato-declares-space-operational-domain-but-more-work-remains/.

evolution of NATO's space posture are the establishment of a new NATO Space Center at Allied Air Command in October 2020 and the creation of a NATO Space Center of Excellence (CoE). The purpose of the Space Center at Allied Air Command is to coordinate Allied space activities, support NATO missions and operations from space, and protect allied space systems by communications sharing regarding potential threats,[22] while the purpose of the Space CoE is to train and educate leaders and specialists from NATO member and partner countries.[23]

Alliance and Individual Members' Attitudes and Posture Toward Space

While NATO's space policy remains classified, its actions, organization, and comments by public officials offer insights into the way the alliance views its role in space. NATO relies on space to enable its operations in all domains and understands the necessity to ensure its ability to execute operations is not interrupted by the intentional or otherwise disablement of space capabilities. However, it has stopped short of declaring space a warfighting domain, unlike the United States. This distinction highlights the current attitudes about space for NATO as an organization. Explicitly declaring space an operational domain in place of a warfighting domain indicates that the focus of NATO in the near- to midterm will be on increasing integration and interoperability among member states. This position closely aligns with public statements made by Secretary Stoltenberg in 2019, when he stated that NATO has no intention of putting weapons in space and will remain purely defensive.[24] As a result, it seems that NATO plans to continue to leverage its space policy and organization to include its newly established Center of Excellence, and to drive requests from alliance members for space-based capabilities designed to enhance military operations. These capabilities include positioning, navigation, and timing (PNT); global communications; missile warning; weather forecasting; intelligence, surveillance, and reconnaissance (ISR); and space domain awareness (SDA).

Furthermore, NATO's space policy and posture represent the collective attitude of the alliance toward space but does not reflect the individual actions undertaken by a number of member states. The United States, France, and, to a lesser extent, the United Kingdom have all indicated its position to view space as a warfighting domain and realign its defense organizations accordingly. The United States recently established a military service dedicated to space, the U.S.

---

[22] Allied Air Command Public Affairs Office, "NATO Agrees New Space Centre at Allied Air Command," ac.nato.int, October 23, 2020, https://ac.nato.int/archive/2020/NATO_Space_Centre_at_AIRCOM.

[23] Christina Mackenzie, "NATO Names Location for New Military Space Center," Defense News (Defense News, February 5, 2021), https://www.defensenews.com/space/2021/02/05/nato-names-location-for-new-military-space-center/.

[24] Martin Banks, "NATO names space as an 'operational domain,' but without plans to weaponize it." *Defense News*, November 19, 2020. https://www.defensenews.com/smr/nato-2020-defined/2019/11/20/nato-names-space-as-an-operational-domain-but-without-plans-to-weaponize-it/.

Space Force, and re-established a unified combatant command, U.S. Space Command.[25] France is following closely behind with France's Minister of Defense detailing the countries plan for establishing a new space force.[26] Lastly, the United Kingdom created a space command in 2020. These actions highlight the growing importance of the space domain to NATO's largest alliance members and are important considerations for the evolution of NATO's space policy.

Threat Environment

NATO has been clear on its view that space exploration and peaceful activities are allowable by any country. Increasingly aggressive states like Russia and China that seek to disrupt the peaceful nature of space, however, are a threat to all government and commercial actors in space. China and Russia have been clear on their stance that disrupting satellites and other dual-use systems is key to subverting U.S. military effectiveness. Russia demonstrated this intent in 2018 by disrupting the GPS signal for NATO allies during Trident Juncture, the largest joint exercise since the end of the Cold War. Both kinetic (*e.g.*, anti-satellite missiles) and non-kinetic (*e.g.*, signal jammers) weapons will have a permanent home in adversary arsenals. Furthermore, there is the potential risk of cyber effects against space systems or equipment. Such an attack could have tremendous effects on GPS systems, banking, universal time, and more.

During a 2020 press conference Secretary Stoltenberg also affirmed that NATO is as much a political alliance as it is a military one and as a result, it should utilize its full diplomatic, economic, and informational strength to tackle the threat posed by hostile actors. By seeking cooperation and the spread of democratic values, NATO can protect the alliance and its fundamental interests while simultaneously determining the risk to its joint military systems. NATO has also reaffirmed its position as a defensive organization, therefore ruling out any NATO weapons' or systems' placement in space.

IV.Models for Comparison

As the nature of warfare has changed, NATO has faced the risk of failing to adapt to new operational domains and tactics. It recognized as much with the cyber domain and is now moving in this direction by recognizing space as well. To help characterize our interview findings and determine policy recommendations for NATO to pursue, we looked at NATO's history with regards to strategic capabilities—the foundation for NATO's creation—and the cyber domain—NATO's most recent example of building out a new domain and developing its policies. Below we have first outlined the history of both the strategic capabilities and cyber models, and then conducted a comparison against our recent interview findings. By doing so, we found particular

[25] *See* Raymond, John. "Space Capstone Publication." U.S. Space Force, June 2020. https://www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf.

[26] Arthur Laudrin, "France's 'Strategic Autonomy' Takes to Space." *International Institute for Strategic Studies*, August 14, 2019. https://www.iiss.org/blogs/military-balance/2019/08/france-space-strategy.

similarities and differences between space and these two models which then helped with our formation of policy recommendations.

Cyber Model

NATO's Allied Joint Doctrine for Air and Space Operations outline the ways in which NATO-forces employ space-based capabilities in support of its primary mission of protecting freedom for its member states. Specifically, the doctrine outlines how NATO leverages space assets of its member states to support operations in land, air, sea, and cyber domains. NATO first confirmed a cyberattack would trigger collective defense in 2014, and later recognized cyber as a warfighting domain in 2016. NATO Secretary General Jens Stoltenberg continues to assert the implications for Article V, stating "A serious cyberattack could trigger Article V, where an attack against one ally is treated as an attack against all."[27] Despite having been recognized as a domain for almost three years, NATO has yet to publicly declare how an attack on space capabilities might trigger collective defense.

In the event of a cyberattack, the victim country needs to decide whether, under the United Nations Charter, the use of force in self-defense would be legal. The result of the 2007 cyberattacks on Estonia initiated an internal cyber assessment of their cyber security and infrastructure defenses alongside the establishment of a cyber defense policy and the creation of the NATO Cooperative Cyber Defence Center of Excellence (CCDCOE).[28] The Tallinn Manual has worked to provide a global norm in cyber space by applying existing international law to cyber warfare. The manual suggests that states do not have sovereignty over the Internet, but that they do have sovereignty over components of the Internet in their territory. A common approach to cyber defense is still missing, thus dividing NATO members that pursue a more active defense—the United States, the United Kingdom, and France—and those that prefer a more defensive approach—Germany and Spain. The United States, The United Kingdom, and France view cyber defense and deterrence as ensuring not only a responding strike in the event of a cyber-attack, but also the possibility of a preventive action against potential adversaries. Germany and Spain envision cyber deterrence as a country's ability to promptly and adequately respond to a cyber-attack, enacting what is defined as hack-back. Since 2019, some member states such as the United States, the United Kingdom, France, Denmark and Estonia have made significant strides in agreeing on a NATO framework within which they are willing to integrate voluntary contributions in terms of defensive and offensive operations.[29] In the age of globalization, interdependence, and digital interconnectedness, states must engage in increased

[27] NATO, "NATO Will Defend Itself." NATO, 27 August 2019. "https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en."

[28] Kohler, K. "Estonia's National Cybersecurity and Cyberdefense Posture." *Center for Security Studies*, September 2020, css.ethz.ch.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-forsecurities-studies/pdfs/Cyber-Reports-2020-09-Estonia.pdf

[29] Abdullah K. Al-Saud, "Cyber Defence in NATO Countries: Comparing Models." *Istituto Affari Internazionali*, 05 February 2021, https://www.iai.it/sites/default/files/iaip2105.pdf

cooperative cyber defense activities to counter and prevent devastating Internet attacks and their implications.

NATO currently provides a crucial cyber defense/response support with oversight from the Cyber Defence Committee. At the operational level, the Cyberspace Operations Centre (CYOC) within the Allied Command Operations (ACO) in Mons, Belgium, is responsible for monitoring and coordinating NATO cyber operations to include the coordination of cross-domain operations in the land, maritime and air domains. At the technical level, the National Cyber Security Center (NCSC) and NATO Computer Incident Response Capability (NCIRC) provides constant monitoring and assistance with response to a cyber-attack event and supports the Cyber Defense Management Board (CDMB). CDMB gives NCIRC a platform for coordinating the swift exchange of information and techniques in relation to cyber-attacks amongst member-states through representatives of military, diplomatic and technical bodies. Additionally, Cyber Reaction Teams are available at the disposal of member countries in the event of a damaging cyber-attack. While the lack of a defined cyber policy is problematic, the efforts thus far to collaborate on cyber issues form a strong model for how NATO should approach space.[30] [31]

Strategic Capabilities Model

Collective defense, crisis management and cooperative security are essential core tasks in support of strategic capabilities for NATO. Under collective defense, members will deter and defend against any threat of aggression including those in accordance with Article V, and emerging security challenges. The core element in the overall strategy of deterrence is based on a mix of nuclear and conventional capabilities. The strategic nuclear forces supporting the deterrence of the alliance are particularly provided by those of the United States which are referred to as the "supreme guarantee" of the security of allies. The United Kingdom and France have a deterrent role of their own by contributing to the overall deterrence and security of the Allies through their independent strategic nuclear forces. Under crisis management, NATO maintains a set of political and military tools to help de-escalate rising crises and consolidate post-conflict stability in response to protecting Alliance security. While through cooperative security, NATO works to enhance international security by developing partnership with relevant countries and other international organizations.[32]

[30] *Ibid.*

[31] Ablon, L., Binnendijk, A., Hodgson, Q., Lilly, B., Romanosky, S., Senty, D., & Thompson, J. "Operationalizing Cyberspace as a Military Domain: Lessons for NATO." *RAND Corporation*, June 2019, https://www.rand.org/pubs/perspectives/PE329.html.

[32] NATO, "Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization." NATO, 20 November 2010, http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

Given the importance of nuclear forces contributing to the overall deterrence and security of NATO, the NPG was created to act as NATO's principal body for planning, discussing, and deciding on matters relating to nuclear policy. This group is composed of the national delegations of all participating Allies with the exception of France. While the North Atlantic Council (NAC) is the ultimate authority, the role of NPG is specifically focused on reviewing Allied nuclear policy in response to evolving international security challenges and adapt changes if necessary. The NPG High Level Group (HPG) acts as the senior advisory body to the NPG concerning the safety, security and effectiveness of NATO's nuclear deterrent. Decisions within the NPG are based on consensus amongst Allies in accordance with all other NATO working groups.[33]

In Comparison to the Cyber Domain

The development process of cyber as a NATO military domain offers numerous insights that can be used for the space domain. For example, the establishment of a cyber defense organization within the NATO command structure and the lessons drawn from that informed how NATO set up the space center and air command. Lessons can be extrapolated from a technical level from the cyber experience. In policy terms, the concept, importance, and complexity of attribution is similar in both the cyber and space domain. An interesting similarity worth considering is the role private sector actors play in the space and cyber domains.

NATO has also made it clear that a defensive posture for cyber is insufficient. NATO must reserve the ability to counter a cyber attack within the same domain, or by using kinetic tools. Since only several members have robust cyber attack capabilities and they are jealously protected—a similarity, in fact, to the space domain and current capabilities— it is challenging to demonstrate political oversight or equal stakes in a response. How can the different representatives vote yes on a cyber counter-strike if they are not aware of what the response will entail? Similar considerations are inherent for the space domain.

In the same vein, however, it is important to recognize the differences between the two domains. Space has more of an international legal framework than cyber. Direct and indirect treaties provide a framework for conduct in space more so than in cyber. It does not mean that adversaries will not try to get around the legal framework for space interaction in the same way that cyber is seen as a gray area. Additionally, there is an aspect of space that is cleaner than cyber due to the physicality of the space domain.

The international management of the domain is an area worth looking into as well. The ITU is part of the United Nations family, but NATO's Cooperative Cyber Defense Center of Excellence engages with the ITU and the lessons learned from the interaction between NATO and the ITU on cyber-related issues might be worth exploring.

---

[33] NATO, "Nuclear Planning Group (NPG)." NATO, 27 May 2020, https://www.nato.int/cps/en/natolive/topics_50069.htm.

In Comparison to the NATO Strategic Capabilities Concept

While there are a number of stark differences between the space domain within NATO and NATOs strategic capabilities concept, there are common elements worth comparing to inform the evolution of the space domain. Most notably, lessons can be drawn from how NATO utilized the NPG to add flexibility for the alliance in developing policy and guidelines for NATO defense plans and programs relating to nuclear weapons. With such asymmetric alliance member strategic capabilities, NATO relied on its highly capable members to lead discussions on policy and doctrine through the NPG. While space capabilities are proliferating to member states, the United States, France, and the United Kingdom all maintain far superior space capabilities and more mature civil and military space sectors. NATOs flexibility and organizational structure designed to leverage the assets and expertise from nuclear-capable states could, potentially, be applied to the space domain.

Redundant safety and security measures designed to prevent accidental or unnecessarily escalatory military capabilities are vital to both nuclear and space deterrence. Within NATO, the military committee provides consensus-based advice to the NPG and NAC, thus allowing nuclear-related decisions to be informed by both the military and political structure of NATO. With the prevalence of civil, commercial, and military space sectors and assets, alliance-based space decisions and actions may similarly benefit from being informed by both the military and political structures of NATO.

V. Presentation of Findings

The summarized findings highlight opportunities, limitations, and additional considerations when attempting to extrapolate lessons learned from the cyber domain and NATO's strategic capabilities model.

1. NATO conspicuously lacks an unclassified space posture.
2. NATO is missing the internal structure and cohesion to contribute to norms development.
3. NATO will face funding challenges related to COVID-19 related expenses.
4. NATO lacks a clear understanding of what would constitute an Article V decision.
5. NATO may be forced to reconsider its current posture due to differing member views of space's role.
6. NATO's strength is its capability sharing between members.
7. NATO's information sharing regarding space is more feasible than with other domains, such as cyber.

8. NATO lacks interoperability requirements for member space systems.
9. NATO's past will raise questions of developing its own space systems.
10. NATO will likely be slow in its evolution of the space domain, given its political decision-making process,

NATO conspicuously lacks an unclassified space posture.

Were NATO to release an unclassified version of its space posture, perhaps a modified version of the classified 2019 document, there would be benefits and consequences to consider. The disadvantages lie in the possibility of asymmetrical commitment on behalf of members, especially those that have underdeveloped or no space programs. If a member with a robust space capability is attacked, the willingness of all members to respond is questionable at best. Furthermore, if NATO takes a public stance as to what it considers constitutes an attack in space, increasingly aggressive states like Russia and China will naturally test the redline. As well, political considerations within NATO rest upon the shoulders of multiple leaders who are accountable to their populations. The same leaders could face scrutiny if engaging in a NATO-wide action in response to a space attack the population was unaware existed.

The benefits to releasing a strategy, however, are likely sufficient to overcome any of these foreseen issues. First, leaders can also be accountable to their populations by demonstrating a commitment to peace and security in all domains, especially with the far-flung importance of space-based systems for the everyday citizen. Second, the ability to project and communicate resiliency and second strike capability is key to any deterrence model. In response to existing or future conflict, an unclassified posture release would be a form of strategic communications that NATO's overwhelming concern is maintaining peace in space and forgoing the development of its own weapons and systems. All in all, the fact there is not yet an unclassified policy is a testament to how NATO tends to both over-classify its internal deliberations, as well as how immature the space conversation has been within the alliance.

NATO is missing the internal structure and cohesion to contribute to norms development.

As a norms development and rulemaking role is not codified in NATO's charter, exerting a leadership role in any of the operational domains will be hard to achieve. Through partnerships with multinational organizations like the International Telecommunication Union (ITU), NATO has contributed to guides and strategic planning aides but even within NATO, achieving consensus about alliance norms and policies is very challenging. For example, some members may want exemptions and exemptions built into policies. Some interviewees also went as far to say NATO will not help establish norms in the international arena without facing an existential threat, one with a solution reliant upon the majority of the international community acting in a particular manner befitting NATO. Furthermore, the unanimous nature of NATO decision-making means

that only one member is required to throw off a consensus. While NATO is a primary forum for discussion for its members, extending this influence to the greater international community is not a part of NATO's role.

NATO will face funding challenges related to COVID-19 related expenses.

NATO is already plagued by slow decision-making and member disagreements regarding adequate and equal funding. Given the financial burden that the pandemic has placed on governments and the greater international economy, it is likely that either member funding will decrease or that member states will continue to struggle with meeting their financial commitment to the alliance. Leaders will face pressure to limit defense budget increases in order to use funds for economic recovery. Since space is not yet at the forefront of NATO concern, spending on these endeavors will naturally be pushed to the margin and existing programs will be funded in their place. For an evolving domain, this can be debilitating.

NATO lacks a clear understanding of what would constitute an Article V decision.

Ambiguity is inherent in the entire concept of NATO. If there is an armed attack on a member state, all member states must come to help. It is the definition of collective defense. However, there is a caveat that says each state will decide what they will bring to the table based on what they think is appropriate. Consequently, remaining ambiguous regarding when, how, and if an attack on space would trigger Article V is at the foundation of NATO's deterrence policy. The ambiguity is also intentional. Aggressors must believe NATO may possess the intent to respond, but will do so in a form, resolve, and timing that most benefits the alliance. For example, if NATO were to announce a threshold stating an armed attack would include the destruction of at least ten satellites, an aggressor might feel motivated to try and destroy nine. As seen through various redlines drawn by individual governments, aggressors will seek to push the threshold, but not surpass it. Given the added ambiguity of an immature space domain, it is even more important that NATO keeps its deliberations largely flexible.

Additionally, there is a difference between the spirit and letter of Article V that is worth considering. The only time NATO has triggered Article V was in response to the September 11, 2001 attacks. This action demonstrated the alliance's resolve to respond to an attack on a member, even if outside of the Europe-focused area of NATO responsibility. And NATO's actions in absence of a formal Article V invocation, as seen in Syria and Ukraine, highlights the resolve of the alliance regardless of formalities. A range of response options available to NATO allows for added flexibility.

An final consideration in the collective defense concept as applied to space versus other domains is the impact of kinetic weaponry. Employing a kinetic weapon in the air, land, or sea domains typically ends in the loss of human life and physical damage. Political willingness to achieve consensus on Article V is a lot easier for physical damage. If a hostile actor starts interfering or attacking in space, the political will of alliance members to respond in kind might be

much lower than if the same were true in more traditional domains (*i.e.*, air, land, and sea). Depending on how an attack in space unfolds, there will be no immediate or direct loss of life, satellites might be temporarily or permanently damaged, and thus have differing effects on NATO member countries, but still much harder to demonstrate the direct and dire consequences the attack had on the alliance. As a result, it will be harder to get to action toward collective defense responses.

That does not mean NATO cannot prepare itself for a situation in where Article V would be invoked, or the alliance would undertake collective defense measures, and build plans to effectively respond. To develop a comprehensive plan to respond to aggressive or hostile action in space, it is potentially easier to have fewer members with similar capabilities. With fewer countries creating a plan, getting to a position where you can say yes and present options to leadership is important. That may be a way to advance NATO's space policy, in a similar vein to what was done in the 1960s with the NPG concept.

NATO may be forced to reconsider its current posture due to differing member views of space's role.

NATO needs to discuss whether space is of vital importance, or simply serves in an enabling function. Currently, NATO views space as a vital component to its multi-domain operations - its primary purpose is to strengthen operations in the air, land, and sea domain and it reinforces nearly every NATO operation in those traditional domains. There is a school of thought that the more one views space as its own warfighting domain, the more risk there is to losing sight of the multi-domain/joint all-domain approach. Alternatively, with the evolving nature of space, a dedicated focus on space as a separate warfighting domain may posture NATO for the mid-to-long term realities of the domain. The United States has taken a more deliberate approach to viewing space as a separate warfighting domain where independent military options in, to, and from space are developed and potentially leveraged to advance national security. As more alliance members, to include France and the United Kingdom, take actions that more closely reflect the United States' current position, NATO will need to engage in deliberate dialogue to determine if its posture toward the domain will remain or if it will evolve to mirror the posture of its more aggressive members.

NATO's strength is its capability sharing between members.

For countries with robust space programs, there are clear advantages to sharing and contributing capabilities within a multinational organization like NATO. For example, the United States faces consistent pressure from Russia and its determination to pursue counterspace technologies that would severely harm U.S. interests. The United States could leverage NATO to offset some of the pressure put on them by Russian counterspace threats and perhaps increase its resilience and deterrence options. Alternatively, if there were an attack, one could leverage Article V but members have to be willing to share what is happening, particularly the United States—it has to provide alliance members (high and low capability states) with the appropriate situational

awareness. If it is technically infeasible to share information, or a country with highly capable space assets chooses not to share for political or military reasons, that could seriously undermine the alliance and could serve as a tool an adversary or hostile actor could use to drive a wedge between alliance members. Information and capability sharing in the space domain, strategically and tactically, needs to be a key tenet of NATO's space policy moving forward.

Sharing information regarding space is more feasible than with other domains, such as cyber.

It is not as challenging to share information regarding the space domain as it is in the cyber domain. Space situational awareness, and the participating institutions that inform it, was built to act as a more open forum. For example, once the United States developed technology to track space orbital debris, it shared the knowledge with the international community. The United States has helped other nations in space, including China, and are willing to share knowledge where there are vulnerabilities. A reason for this openness could be tied back to the fundamental understanding of the harm space debris can have on space assets. The nature of the domain influences the willingness of countries to share. It is mutually beneficial for a state with space debris tracking to alert an ally or an adversary if it is in immediate danger of being struck by a piece of inactive space debris, as not doing so would increase the amount of indiscriminate orbital debris capable of damaging space assets, regardless of country ownership. Additionally, unlike cyberspace, a certain amount of domain awareness comes from ground-based telescopes that are proliferating to non-military space sectors. With space, it is a lot easier for the United States. to share and let actors know what is going on up there. It is not as compartmentalized or classified as other areas.

NATO lacks interoperability requirements for member space systems.

NATO has a joint doctrine/training command and that drives interoperability and information sharing requirement development for the majority of its operations. But to facilitate advanced doctrine development and training requirements for domains or concepts that require advanced expertise and additional resources, NATO has created a Center of Excellence (CoE) concept. For example, after two years in Afghanistan, a decision was made to establish a special forces CoE. The space domain is a particular area where the CoE could drive interoperability requirements, but mostly around information sharing. It is unlikely that NATO, or the CoE, would play a significant role in developing interoperability requirements for state-owned space capabilities. The alliance relies on membership contributions but does not dictate what technical requirements are associated with alliance member's space capabilities. With that in mind, NATO does play a significant role in the development of standards and protocols that typically go up to joint doctrine command. After NATO starts to push out doctrine based on standard protocols, there is a trend that nations, both alliance members and strategic partners to NATO, start to adopt them.

Information sharing and interoperability of space assets does have many different aspects worth considering. There are space-related interoperability/information requirements that have been developed for years within the alliance. Specifically, the defined contributions of space assets to ballistic missile defense, joint ISR, and GPS have matured over the years. So there is a

precedence of NATO driving interoperability and information sharing among alliance members. There is not a clear understanding of whether NATO will establish or publish standards for satellites in general. The evolution of space policy brings a need to expand information sharing requirements with more space domain specific assets. The output formats, details, and standardization of information needs to be similar in order to fully leverage alliance members contributions and more readily transfer from ally to ally or command to command. The role of the space center is critical here and will play a key role in fusing information generated from allied members' organic space capabilities and transfer it through the right NATO channels and to the field. Enhanced fusing and dissemination of information is the best way NATO can leverage contributions from alliance members and where interoperability and standardization comes into play for space.

NATO's past will raise questions of developing its own space systems.

By the early 2000s, it was clear that there was better value and better results if the alliance leveraged individual member states contributions instead of having a NATO owned replacement satellite developed to replace the NATO 4A and 4B satellites. The operational environment had changed significantly since NATO developed SATCOM satellites. With more alliance members generating organic space capabilities and NATO having scarce resources, it was a strategic decision in the early 2000s that remains true today. There have not been any significant problems with the current framework. The needs of NATO with regards to leveraging space capabilities to enable operations in other domains are being met by the contribution of allies. It is difficult to predict whether this will change in the future, given the rapid pace of development, but it is unlikely in the foreseeable future that NATO will pursue the development of any space-related capabilities.

Given its political decision-making process, NATO will likely be slow in its evolution of the space domain.

NATO and its member states have experience as to how crippling cyber can be. Notably, Estonia suffered a massive cyber attack in 2007, the United States has experienced cyber attacks on a number of occasions, and NATO has been subject to attacks on personnel in the Baltics and Poland. These cyber attacks have led to declarative statements in a number of multinational organizations, to include the United Nations. Senior advisors at the U.S. State Department outlined how cyber-attacks could reach the level of damage/destructiveness that would warrant retaliation under Article 51 of the United Nations Charter (self-defense). There is an argument to be made that if an actor was attacked under the definition of international law, military force could be justified and necessary in response. NATO outlined this formally saying cyber could threaten sovereignty and integrity of the member state and if sufficient enough damage, Article V could be triggered. The ability of NATO to unambiguously state that a cyber attack could trigger Article V and that nuclear weapons could be employed was predicated on the widespread understanding of cyber attacks on alliance members. At this moment, alliance members do not have the same

experience in space. One could argue that an attack on space assets of NATO members could be so crippling, that Article V could be triggered and collective response could occur, but gaining concurrence from all alliance members to declare that position right now would be challenging. There is great asymmetry between alliance members space capabilities, a fundamental difference in how alliance members view space (*e.g.*, as a warfighting domain or a shared commons), and there has not been a significant enough space attack to elevate the common understanding of the threats posed by space-based attacks.

VI. Policy Recommendations

The most important section of this research paper consists of the policy recommendations. Drawing upon background research, expert knowledge, and comparative analysis, the following recommendations are comprehensive in nature and address the main problems plaguing NATO in the beginning years of its buildout of the space domain. Discussion of these recommendations also includes considerations of the risks and/or hardships associated with their implementation.

1. NATO should ensure its flexibility in response is codified in future space policies.

In order to maintain flexibility in response while ensuring it has an adequate deterrent in place, NATO must provide an adaptive or open-ended redline in its unclassified space policy. As seen in recent years, drawing a redline in advance of, or during, conflict can be detrimental to government leaders and administrations. Establishing a policy that outlines a particular action as a surefire provocation for a response is warranted in extremely complex situations, but the failure to uphold the terms of said redline can then cause large credibility issues for the government or leader that initially issued the redline. If deterrence is described as the clear signaling of capabilities and the intent to respond to a particular course of action by an adversary, neglecting to follow through can be disastrous and ultimately lead to further threats of conflict further down the line. Instead of being deterred, adversaries are emboldened and will seek to test a country or alliance's resolve in other areas.

For this reason, NATO must adopt a flexible response redline similar to what it has in place for attacks in the cyber domain. As the boundaries of space conflict are explored in the coming decades, NATO must not limit itself to a certain threshold of response. If NATO were to explicitly state what degree of attack severity or type it considers worthy of triggering collective defense discussions, then adversaries will know that below that line, NATO is unlikely to respond as an alliance. Therefore, NATO's broader peace and security will face a larger threat. Gauging the severity of particular attacks will also be challenging, a reason why the strategic capabilities model is not the best foundation for this model. As opposed to the use of nuclear weapons and a clear, severe threshold of attack, both cyber and space can range from small interruptions to full-flown virtual and/or physical destruction. NATO must reserve the ability to respond in kind, and it is vital that it allow itself the freedom to determine what does and does not constitute an attack.

2. NATO should establish a Space Planning Committee to guide its efforts in the domain.

NATO should stand up a Space Planning Committee, mirrored after the NPG construct leveraged to guide its strategic capabilities policy. The NPG was proposed by Robert McNamara in early 1960 as a way to develop policy and guidelines for NATO defense plans and programs relating to nuclear weapons. In his statement justifying the need for an NPG, McNamara indicated that alliance members' nuclear forces combined were numerically larger than the Soviet Unions, the survivability of the alliance's strategic weapons were greater when combined, and it allowed for added flexibility.[34] The NPG would act as a senior body on nuclear matters for the alliance, allowing NATO to rapidly adapt policy to maintain the nuclear advantages of the alliance regardless of new developments. Inaugurated in 1967, the NPG continues to serve as a senior body on nuclear matters in the alliance. A similar concept should be implemented for the space domain, albeit at the committee level of NATOs organizational structure.

While strategic and space capabilities are markedly different, the fundamental reason for the establishment of NPG serves as a potential model for managing space policy within NATO. NATO alliance members collectively own approximately 50 percent of all orbiting satellites.[35] Additionally, the capabilities individual countries possess range from domain enhancing functions, like ISR and GPS, to domain-specific advanced warfighting functions, like orbital warfare and space electronic warfare. A Space Planning Committee within NATO would more appropriately leverage the expertise of alliance members across the entire spectrum of engagement.

While a NATO official will serve as the lead for the Space Planning Committee, a small group of leading space alliance members including the United States, France, and the United Kingdom should serve as primary advisers and leading advocates. Forming an NPG-like committee that reports directly to the NAC that guides the evolution of space policy will allow NATO to more rapidly respond to the quickly evolving domain by leveraging highly capable alliance members expertise while providing an opportunity for lesser capable alliance members to contribute to the discussion and enhance their understanding of the space domain. To achieve NATO's near-term goal of maintaining a defensive posture in space, enhancing joint all domain command and control, and maintaining space as a global commons, NATO should leverage the newly developed Space CoE to evolve interoperability standards and cross-domain information sharing. But to better posture the alliance to respond to potential hostile, kinetic, or non-kinetic actions in, to, and from space by adversaries, the committee should focus its time and resources on the development of alliance-specific space warfighting doctrine, discussion of alliance members

[34] Sayle,Timothy Andrews. "A nuclear education: the origins of NATO's Nuclear Planning Group," *Journal of Strategic Studies*, 43:6-7, 920-956, September 10, 2020. DOI: 10.1080/01402390.2020.1818560

[35] NATO, "NATO's Approach to Space." NATO, October 9, 2020. https://www.nato.int/cps/en/natohq/topics_175419.htm.

strategic space posture, and Article V considerations for the space domain, all of which mirror the earliest agenda items of the NPG in the 1960s.[36]

3. NATO should expand its partnerships with international entities and the private sector.

NATO should adopt a policy of defining the relationship between NATO space elements and multinational partner entities and industry/private sector actors, comparable to NATO's cyber defense model. Within NATO, the cyber defense policy defines and codifies the important relationship between NATO and strategic partners, like the UN, and industry/private sector actors to influence the cyber domain. Specifically, NATO's CCDCOE maintains a relationship with the ITU. The ITU, a United Nations specialized agency, is a recognized body that facilitates international connectivity in communications networks, allocates radio spectrum frequency and satellite orbits, and develops technical standards to ensure networks and technologies seamlessly connect.[37] The union has membership from 193 states and upwards of 900 companies, universities, and international and regional organizations. NATO's CCDCOE recognized the important role the ITU played in facilitating global communications and overtly cooperated with the ITU to co-author the National Cybersecurity Strategy Guide. NATO's space elements, to include its new Space CoE, should develop similar partnerships with multinational organizations involved in the management of the space domain. Initially, the Space CoE should partner with existing multinational organizations like the ITU and the United Nations' Office for Outer Space Affairs. While these organizations are not focused on military space, the dual-use nature of space capabilities warrants NATO's participation with and in international space partnerships.

Similarly, NATO space policy should specifically cultivate a relationship with industry partners, in the same vein as the NATO Industry Cyber Partnership (NICP). There is a noticeable difference between NATO's cyber defense and space, in that NATO is required to defend its organic cyber networks. NATO does not own, nor plans to develop, organic space capabilities and relies on alliance members to protect their own capabilities. Despite this difference, NATO should leverage industry partners' evolving competences to augment and enhance the alliance's space capabilities, interoperability, and information sharing. In the near term, NATO should develop an industry forum designed to foster dialogue between alliance members and industry partners for the purpose of evolving joint, all-domain command and control. As NATO's space policy matures, the industry partnership could be leveraged to increase space domain awareness within the alliance, augment necessary space capabilities, and increase resiliency among alliance members.

---

[36] Van Eekelen, Wim. "Fifty Years of Nuclear Planning: How It Started." *Atlantisch Perspectief* 41, no. 6 (2017): 42-47. Accessed April 05, 2021. https://www.jstor.org/stable/48581393.

[37] Cordell, Kristen. "The International Telecommunications Union: The Most Important UN Agency You Have Never Heard Of," Center For Strategic and International Studies, December 14, 2020. https://www.csis.org/analysis/international-telecommunications-union-most-important-un-agency-you-have-never-heard.

4. NATO should rely on its Centers of Excellence to drive policy and interoperability innovation.

NATO should look to expand space domain integration in NATO-accredited CoEs and evolve the Space Center of Excellence to establish joint doctrine and set standards for information and interoperability as necessary. CoEs within NATO play a crucial role in furthering innovative ideas, doctrine, lessons learned, education and training, concept and capability development amongst allies through recommendations and experimentation.[38] Within each Center's area of expertise or domain these international military organizations act as hubs amongst Allies and partners members to improve interoperability and capabilities. NATO-accredited CoEs have an expanded reach because they are not part of the NATO Command Structure but part of a wider framework supporting NATO Command Arrangements (NCA), giving CoEs greater flexibility in the relationships with other international and civilian entities.[39] CoEs do not have to abide by NATO policy when performing their research and providing a final product to participating entities.[40] The involvement of participating nations in CoEs bring added value to not only NATO but the key stakeholders and involved nations as well in furthering doctrine development and standardization, concept development and experimentation, education and training, or lessons learned management in relation to the space domain. After NATO starts to push out doctrine based on standard protocols, nations start to adopt them even if they are not NATO members. Thus it is vital that the space domain is integrated into the relevant existing, accredited CoEs. Particular CoEs worth integrating, or further integrating, with space expertise include the Cold Weather, Command and Control, Cooperative Cyber Defense, Modeling and Simulation, and Integrated Air and Missile Defense CoEs.

Furthermore, the fundamental reason for the expansion and evolution of the Space CoE is to strengthen protocols and interoperability amongst entities. CoEs have proven to be successful models in several areas in relation to multinational solutions to enhance capabilities and capacities. For example, as a result of establishing the NATO CCDCOE took a valuable initiative in creating and continuously updating a manual for managing cyberwar, the Tallinn Manual. As such, the Space CoE should look to the CCDCOE as a roadmap for the types of products it should focus on in the early years of operations. A space law toolkit, in the same spirit as the cyber toolkit developed by the CCDCOE, could be developed to detail the existing legal framework guiding the behavior space domain. Given the many different aspects of the space domain, the evolution and expansion of the Space CoE will provide a strong foundation as a hub for the increased dissemination of information in support of joint doctrine and interoperability.

---

[38] NATO. (n.d.). Retrieved April 09, 2021, from https://www.act.nato.int/centres-of-excellence

[39] NATO, "Centres of excellence." NATO, 20 April 2018, https://www.nato.int/cps/en/natohq/topics_68372.htm

[40] CHIPS articles: NATO centers of excellence. (n.d.). From https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=6226

VII. Conclusion

Despite the uncertainty surrounding the future of conflict and how theories of victory and warfighting play out in the space domain, NATO's introduction of space as a new operational domain presents a world of opportunity for the alliance. Stemming back to the fielding of NATO's own satellite in the early 1970s, space has either served as an independently driven domain or as an enabler of warfighting in other domains. As the international onus is put on the development of robust space capabilities as a potential precursor to military successes in the future, NATO must jump ahead of the curve and publicly state its policy for the domain.

Again, the bureaucratic challenges that come naturally with an organization of this size must be pushed aside for NATO to release an unclassified space policy as soon as possible. This policy should codify NATO's intent with regards to the fielding of its own space capabilities, its acceptable thresholds and playbook of deterrence and response, and lastly its desires for the domain. NATO must continue recognizing the unique, borderless challenges promulgated by the space domain and be cautious while publicly stating its acceptable thresholds of actions by hostile parties. Furthermore, NATO must affirm its ability to adapt this threshold whenever possible in response to the increasing congestion and competitiveness of space.

By creating a Space Planning Committee, NATO members with key space capabilities will have a smaller forum to deliberate and plan various policy or operational concepts and then present them for consideration to the larger alliance. Key considerations of interoperability requirements, capability sharing, and new doctrine can occur within this space. Closely tied to this is the importance of collaborating with other international bodies and industry partners, both of whom represent opportunities vital to NATO's future within space. While NATO is not an international norm-making body, it must emerge as a key proponent of maintaining peace, stability, and security whenever possible. Lastly, evolving the new space CoEs and integrating space expertise and awareness into existing COes will demonstrate yet another step towards increasing the dialogue on space issues.

Although this paper does not seek to solve all of the challenges associated with NATO's operationalization of space, it is meant to inspire further discussion of these issues within the national security community. Just as the understanding of future space conflict and possible scenarios matures, so too must the assessment of what deterrence and NATO's future will consist of within the domain. There is no room to delay.

APPENDIX A: Interviews

Date	Name	Organization
3/5/2021	Kestutis Paulauskas	NATO Action Officer
3/5/2021	Robert Bell	Senior Civilian Representative of the Secretary of Defense in Europe (SECDEFREPEUR); Defense Advisor (DEFAD) to the U.S. Ambassador to NATO
3/12/2021	Benjamin Bahney	Space Program Leader - Lawrence Livermore National Laboratory
3/16/2021	Sarah Tarry	Director - Operational Preparedness Section, Operations Division, NATO
3/18/2021	ADM. Michelle Howard (ret.)	Commander - Allied Joint Force Command Naples

Bibliography

1. Al-Saud, Abdullah K. "Cyber Defence in NATO Countries: Comparing Models." *Istituto Affari Internazionali,* 05 February 2021, https://www.iai.it/sites/default/files/iaip2105.pdf

2. Banks, Martin. "NATO names space as an 'operational domain,' but without plans to weaponize it." *Defense News,* November 19, 2020. https://www.defensenews.com/smr/nato-2020-defined/2019/11/20/nato-names-space-as-an-operational-domain-but-without-plans-to-weaponize-it/.

3. Binnendijk, Ablon, L., A., Hodgson, Q., Lilly, B., Romanosky, S., Senty, D., & Thompson, J. "Operationalizing Cyberspace as a Military Domain: Lessons for NATO." *RAND Corporation*, June 2019, https://www.rand.org/pubs/perspectives/PE329.html.

4. CHIPS articles: Nato centers of excellence. (n.d.). From https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=6226

5. Cordell, Kristen. "The International Telecommunications Union: The Most Important UN Agency You Have Never Heard Of," Center For Strategic and International Studies, December 14, 2020. https://www.csis.org/analysis/international-telecommunications-union-most-important-un-agency-you-have-never-heard.

6. Defense Intelligence Agency. "Challenges to Security in Space," DIA, January 2019. https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf.

7. Garcia, Mark. "Space Debris and Human Spacecraft." NASA. NASA, April 14, 2015. https://www.nasa.gov/mission_pages/station/news/orbital_debris.html.

8. Harrison, Todd, and Kaitlyn Johnson. "Space Threat Assessment 2021." Space Threat Assessment 2021 | Center for Strategic and International Studies, March 31, 2021. https://www.csis.org/analysis/space-threat-assessment-2021.

9. Harrison, Todd, Zack Cooper, Kaitlyn Johnson, and Thomas G. Roberts. "Escalation and Deterrence in the Second Space Age." Center for Strategic and International Studies, October 2017. https://csis-website-prod.s3.amazonaws.com/s3fspublic/publication/171109_Harrison_EscalationDeterrenceSecondSpaceAge.pdf?pkaq8A3h5rRj8zkOrL2bDpUa4MtjERPa.

10. Hennigan, W.J. "Strange Russian Spacecraft Shadowing U.S. Spy Satellite, General Says." *Time Magazine,* February 20, 2020. https://time.com/5779315/russian-spacecraft-spy-satellite-space-force/.

11. IISS. “An Introduction to Russia's Military Modernisation.” IISS, September 2020. https://www.iiss.org/blogs/analysis/2020/09/rmm-introduction.

12. Kohler, K. “Estonia’s National Cybersecurity and Cyberdefense Posture.” *Center for Security Studies,* September 2020, css.ethz.ch.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-forsecurities-studies/pdfs/Cyber-Reports-2020-09-Estonia.pdf.

13. Laudrin, Arthur. “France’s ‘Strategic Autonomy’ Takes to Space.” *International Institute for Strategic Studies*, August 14, 2019. https://www.iiss.org/blogs/military-balance/2019/08/france-space-strategy.

14. Legendra, Helena. “China's Pursuit of Advanced Dual-Use Technologies.” IISS, December 18, 2018. https://www.iiss.org/blogs/research-paper/2018/12/emerging-technology-dominance.

15. Livingstone, David, and Patricia Lewis. *Space, the Final Frontier for Cybersecurity?* Harrogate, U.K. Chatham House, 2016. Https://Www.chathamhouse.org/Sites/Default/Files/Publications/Research/2016-09-22-Space-Final-Frontier-Cybersecurity-Livingstone-Lewis.pdf.” Chatham House, September 22, 2016.

16. Moltz, James Clay.“*The Politics of Space Security: Strategic Restraint and the Pursuit of National Interests*,” 82–123. Stanford, CA: Stanford University Press, 2019.

17. NATO, “Approche De L'OTAN Concernant L'espace.” NATO, October 9, 2020. https://www.nato.int/cps/fr/natohq/topics_175419.htm?selectedLocale=en.

18. NATO, “Centres of excellence.” NATO, 20 April 2018, https://www.nato.int/cps/en/natohq/topics_68372.htm

19. NATO, “NATO's Approach to Space.” NATO, October 9, 2020. https://www.nato.int/cps/en/natohq/topics_175419.htm.

20. NATO, “NATO, We Have Lift off!” NATO. https://www.nato.int/cps/us/natohq/declassified_138278.htm.

21. NATO, “NATO Will Defend Itself.” NATO, 27 August 2019. “https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en.”

22. NATO. (n.d.). Retrieved April 09, 2021, from https://www.act.nato.int/centres-of-excellence

23. NATO, “Nuclear Planning Group (NPG).” NATO, 27 May 2020, https://www.nato.int/cps/en/natolive/topics_50069.htm.

24. NATO, “Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization.” NATO, 20 November 2010, http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

25. NATO 1, 2017. http://www.astronautix.com/n/nato1.html.

26. O'Rourke, Ronald, and Michael Moodie. 2018. *U.S. role in the world: background and issues for Congress*. CRS Reports (Library of Congress. Congressional Research Service). https://purl.fdlp.gov/GPO/gpo112404.

27. Paulauskas, Kestutis. “Space: NATO's Latest Frontier.” NATO Review. NATO, March 13, 2020. https://www.nato.int/docu/review/articles/2020/03/13/space-natos-latest-frontier/index.html.

28. Raymond, John. “Space Capstone Publication.” U.S. Space Force, June 2020. https://www.spaceforce.mil/Portals/1/Space%20Capstone%20Publication_10%20Aug%202020.pdf.

29. Sayle, Timothy Andrews. “A nuclear education: the origins of NATO’s Nuclear Planning Group,” *Journal of Strategic Studies*, 43:6-7, 920-956, September 10, 2020. DOI: 10.1080/01402390.2020.1818560

30. U.S. Department of State. *Strategic Deterrence Initiative*, January 2009. https://2001-2009.state.gov/r/pa/ho/time/rd/104253.htm.

31. Van Eekelen, Wim. "Fifty Years of Nuclear Planning: How It Started." *Atlantisch Perspectief* 41, no. 6 (2017): 42-47. https://www.jstor.org/stable/48581393.

32. Wall, Mike. “Iran Launches Its 1st Military Satellite into Orbit: Reports,” Space.com (Space, April 22, 2020), https://www.space.com/iran-launches-first-military-satellite.html.

33. Zissis, Carin. “China's Anti-Satellite Test.” *Council on Foreign Relations*, February 2010. https://www.cfr.org/backgrounder/chinas-anti-satellite-test.