OPEN
PUBLICATIONS

Day Zero Integration and Multi-Domain Operations

Volume 11, Number 1, 2025
ISSN 2957-7160 (Online)
ISSN 2957-7799 (Print)

DISCLAIMER:

OPEN publications are produced by Allied Command Transformation/Strategic Plans and Policy; however OPEN publications are not formal NATO documents and do not represent the official opinions or positions of NATO or individual nations. OPEN is an information and knowledge management network, focused on improving the understanding of complex issues, facilitating information sharing and enhancing situational awareness. OPEN products are based upon and link to open-source information from a wide variety of organizations, research centers and media sources. However, OPEN does not endorse and cannot guarantee the accuracy or objectivity of these sources. The intellectual property rights reside with NATO and absent specific permission OPEN publications cannot be sold or reproduced for commercial purposes. Neither NATO or any NATO command, organization, or agency, nor any person acting on their behalf may be held responsible for the use made of the information contained therein. The views expressed in this article are solely those of the authors and may not necessarily represent the views of NATO, Allied Command Operations, or Allied Command Transformation, or of their affiliated organizations. All rights reserved by NATO Allied Command Transformation Open Perspectives Exchange Network (OPEN). The products and articles may not be copied, reproduced, distributed, or publically displayed without reference to OPEN.

Let us know your thoughts on "Day Zero Integration and Multi-Domain Operations " by emailing us at:
editor@openpublications.org

www.openpublications.org

CREDITS

CONTRIBUTING AUTHORS

Dr. Adam Knight
Notre Dame of Maryland University, Assistant Professor
Department of History and Political Science

OPEN CAPABILITY LEADER

COL Stefan Lindelauf

OPEN LEAD EDITOR

Mr Jeffrey Reynolds

OPEN OPERATIONS MANAGER

COL Alexios Antonopoulos

ACTION OFFICER

CDR Aaron Arky

OPEN EDITORIAL REVIEW BOARD

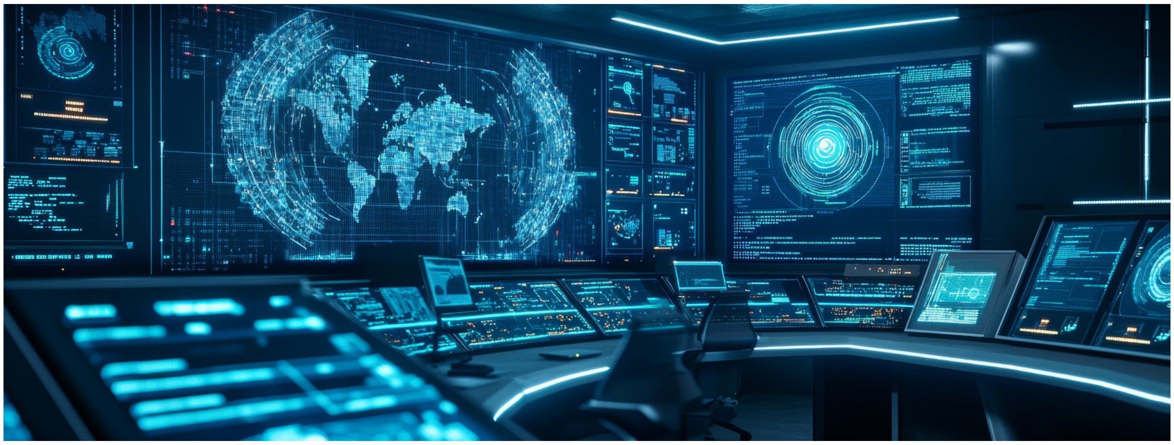
LTC Tor-Erik Hanssen
CDR Alan Cummings
LTC Claus Slembeck
LTC Anders Wedin
LTC Gabor Farkas
LTC Emmanuel Senoussi
LT CDR Cem Caglayan
MAJ Ante Milas
Dr Bohdan Kaluzny
Ms Klodiana Thartori
Ms Jedidja Van Keulen
Mr Helmar Storm
Mr Theodore Rubsamen
Mr Christopher Hall
Mr Benjamin Davenport
Mr Eric Thompson

TECHNICAL EDITOR

Dr. Maureen Archer

ART DESIGNER

PO1 Emilia Hilliard



CONTENTS

ABSTRACT
DAY ZERO INTEGRATION AND MULTI-DOMAIN OPERATIONS

ADAM KNIGHT

After examining two episodes from the Alliance's history of adaptation, this paper describes NATO's MDO and DZI concepts. It also identifies three opportunities for additional adaptations in service of achieving DZI. First, multinational forces under the Framework Nations Concept (FNC) must proactively address substantial political and legal issues to ensure they can take advantage of their potential to respond immediately to the onset of crises. Second, the Alliance must cultivate networked, organic, non-hierarchical relationships among public and private sector cybersecurity experts, public officials, and private firms to the end of encouraging best practices, publicizing newly discovered vulnerabilities, and creating opportunities for experts to aid small government agencies and firms, especially those related to service provision, in the event of a crisis. Finally, as members and potential adversaries continue to develop warfighting capabilities in space, NATO must clarify its position regarding outer space as a warfighting domain.

Keywords: Multi-Domain Operations, Day Zero Integration, Cyberspace, Space, Multinational Security Institutions

EXECUTIVE SUMMARY

Clausewitzian friction impedes operations large and small from their optimal speed and efficacy. As operations grow larger and more complex, they face ever more opportunities to be hindered in such a way. For this reason, operations across domains with several partners designed to secure objectives quickly must directly address this ever-present and potentially calamitous impediment.

For NATO, achieving Day Zero Integration (DZI) in all aspects related to Multi-Domain Operations (MDO) will demand such contingencies. The Alliance provided a working definition of its MDO concept in 2022, describing it as "the orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to deliver converging effects at the speed of relevance".[1] This level of synchronization and speed requires the Alliance's capabilities be effectively integrated across each of five domains (land, air, maritime, cyberspace, and space) and across Alliance members, but also across the divide between public and private sectors, and among as broad a like-minded group of NATO partners as possible.

This paper examines the Alliance's reactive pattern of adapting to new challenges by cooperating internally and externally as new circumstances emerge, using its experiences in the Balkans as an example. The paper also examines how 2023's NATO-Industry Forum (NIF23), as an account of governments and private sector firms, put aside particular interests in service of delivering help to Ukraine quickly in the wake of Russia's invasion. The paper then describes NATO's MDO concept using the US Army's concept of the same name that informed it, as well as ARF which is applying it. This is followed by a discussion of DZI and the variety of obstacles the Alliance faces in achieving it. Lastly, the paper examines three aspects pertinent to DZI that the Alliance can address in service of achieving this goal.

First, "interstitial" forces, namely multinational forces existing between the national and international organizational level without serving as a rival to either[2] —such as German-Netherlands Corps (1GNC) and the Joint Expeditionary Force (JEF)—show promise in developing the capability to execute MDOs quickly. While the Alliance has taken pains to prepare substantial capabilities to respond rapidly in the event of a conflict, these multinational forces, organized under the auspices of its Framework Nations Concept (FNC) may be able to act effectively either before NATO comes to a consensus or outside of a crisis substantial enough to warrant activating these capabilities. However, forces such as these face substantial practical and political barriers to working in concert.

Second, the domain of cyberspace offers adversaries a multitude of avenues by which they can disrupt the lives of Alliance member populations and the operation of their governments and militaries. This is particularly true of small agencies or offices whose systems may not be especially robust in the face of a determined adversary in cyberspace.

[1] *¨Multi-Domain Operations: Enabling NATO to Out-pace and Out-think its Adversaries" 2022.*

[2] *Flynn 2023, p. 313.*

Third, despite the announcement of the Alliance's intentions regarding the domain of space, aspects of the domain remain somewhat underspecified. The Alliance clearly intends to continue coordinating its space-based capability, leveraging both member state capabilities and the resources private firms bring to the table, but its position on warfighting remains absent.

In each case, lessons regarding mitigating friction inform this paper's recommendations. First, governments—especially of Germany and the United Kingdom—ought to negotiate and clarify the coalitions and purposes of multinational forces such as 1GNC and JEF in the event of a crisis's onset, even at the expense of the ability to create ad hoc "coalitions of the willing" to respond to threats to the Alliance.

Second, the Alliance and its members ought to create means by which public and private sector actors can cultivate organic, non-hierarchical relationships to encourage best practices, distribute up-to-date information regarding newly discovered vulnerabilities, and create opportunities to shore up the cybersecurity capabilities of small firms and local governmental agencies, especially those related to service provision.

Third, regarding the domain of space, the Alliance should clarify its position regarding the deployment and use of weapons systems and countermeasures in space. It may prove prudent to limit or forgo certain systems, but regardless, the Alliance should clarify its position on outer space as a warfighting domain.

INTRODUCTION

History offers few (if any) examples of large fighting forces operating in perfect concert with one another. Clausewitz's notion of friction has many sources, but it can emerge in every moving part of an operation, down to the singular individual.[3] Joint operations multiply the possibilities for friction to impede or prevent success merely by adding additional moving parts. This is exacerbated by interservice rivalries, which can stoke counterproductive competition over resources and compromise strategic considerations.[4] It is also exacerbated by alliances, since allies do not perceive one another's challenges and threats the same. This means that arraying a coalitional force to a single objective will require some negotiation or compromise. [5]

These make NATO's adoption of its Multi-Domain Operations (MDO) concept ambitious and troublesome to implement. In seeking to counter the diffusion of anti-access/area denial (A2/AD) capabilities,[6] the Alliance seeks to leverage capabilities across each of five domains (land, air, maritime, cyberspace, and space) from not just member state militaries and other national instruments of power, but also partner nations, a variety of IOs and NGOs, and actors within academia and private industry.[7] To do so effectively, the Alliance aims to achieve Day Zero Integration (DZI). This means effectively integrating capabilities and actors—internal and external—across all domains and categories before a response proves necessary with the onset of a crisis.

To do so, every effort must be made to reduce Clausewitzian friction across the domains and actors in NATO's MDO concept. As complexity of an operation increases, so too does friction.[8] However, if the Alliance is able to sufficiently streamline interactions between its many moving parts, DZI can allow for immediate reaction to emergent crises. Unfortunately, a multitude of factors appear prepared to delay the Alliance's response to a potential threat or the onset of hostilities. For example, while the Balticonnector gas pipeline's severing triggered a substantial response from Alliance members, not all members agreed regarding the ideal nature and venue of response, with German officials arguing that the British-led response in particular was counterproductive.[9] Moreover, interservice rivalries within the same country may be similarly counterproductive, with each branch competing with the others over resources.[10]

The myriad different capabilities will require coordination and therefore command, but this too creates opportunities for problems. First, command and control (C2) in modern conflicts cannot be resolved with a "one size fits all" solution, but the differentiation of C2 across contexts creates the

[3] *Clausewitz 1989, pp. 119-121.*

[4] *Parshall and Tully 2005, p. 25.*

[5] *McCranie 2021, p. 114; Clausewitz 1989, p. 79.*

[6] *Gilli, Gilli, and Grgić 2025, pp. 73.*

[7] *"Multi-Domain Operations in NATO." 2023; Dekker, Gubbels, and Kaloniatis 2024.*

[8] *Carlson and Gurantz 2022, pp. 67-68.*

[9] *Bond 2024.*

[10] *Johnson 2018.*

[11] *NATO STO Research Task Group SAS-143 2024.*

need for harmonization (C2-H) in MDOs.[11] While the supported/supporting interrelationship (SSI) concept can help in this context, this is further complicated by the introduction of novel battlefields to the traditional realms of land, maritime, and air.[12]

Cyberspace and outer space are newer, less understood battlefields. Policymakers often find themselves needing to use kinetic violence as metaphors for cyberattacks[13] in order to underline their seriousness. Outer space occupies similarly uncertain conceptual space. Despite the establishment of a standalone space-based branch of the United States armed forces, there is concern its nature as a conflictual realm is not broadly accepted.[14] As such, these two domains pose significant challenges to the Alliance's MDO success.

This paper examines opportunities for NATO to work towards achieving DZI. The paper first explores examples from NATO's recent history to identify patterns regarding how the Alliance collaborates internally and externally and how it addresses evolving security challenges, focusing on the Alliance's formative experiences in the Balkans and in observing cooperation between the Ukrainian government and industry in the wake of Russia's invasion. The paper then describes NATO's MDO concept, with special consideration given to DZI's importance and challenge. This examination points to the insufficiency of NATO's previous patterns of adaptation and the necessity to continue seeking out new opportunities to address friction before it manifests, if DZI is to be achieved. From there, the paper identifies three aspects pertinent to the MDO concept in which the Alliance can reduce potential friction in service of DZI: so-called "interstitial" level security institutions, cyberspace as infrastructure, and outer space as a potential realm for warfighting. The paper describes three ways to mitigate this friction; each solution bears important similarities.

The Alliance has shown a remarkable ability to react to new challenges, often incorporating a variety of interlocutors as it does so. These instances are no different—these solutions will require supporting new and extant relationships. However, each of them also requires the Alliance to act before crises regarding these aspects emerge, as NATO's ability to react to them as they emerge will likely be insufficient to resolve such crises optimally. On the other hand, taking proactive steps can prevent potential vulnerabilities from materially delaying the Alliance's effective response to a crisis.

[11] *NATO STO Research Task Group SAS-143 2024.*

[12] *Dekker, Gubbels, and Kalloniatis 2025, pp. 6-8.*

[13]*For example, Sen. Romney described the 2020 Solarwinds hack as akin to "Russian bombers reportedly flying undetected over the entire country" (see: Lin 2020).*

[14] *Galbreath and Reeves 2025, p. 4.*

NATO'S PATTERN OF REACTING, ADAPTING, AND COLLABORATING IN THE FACE OF NEW CHALLENGES

Balkan Proving Ground

NATO's deployment to Kosovo (KFOR) is illustrative of how the Alliance addresses new challenges, specifically how operational experiences produce practical adaptations and new Alliance policy. For instance, KFOR benefited from lessons learned regarding civil-military relations—notably its relationships with NGOs—from its experience in Bosnia. Liaison officers, a program initiated in Bosnia, were frequently used as a means of interaction between KFOR and NGOs in Kosovo. While this did not circumvent all disagreements, it did facilitate the cultivation of personal ties aiding coordination between KFOR and NGOs in a number of instances.[15]

KFOR's reactive approach also helped plant the seed for the adoption of Protection of Civilians (PoC). After his tenure as KFOR Commander, General Klaus Reinhardt remarked not only on the military successes of the force, but also on its role in the daily lives of civilians as a preventative measure against advertent and inadvertent escalation along ethnic lines and for its own sake.[16] Not only would KFOR's experience inform the UN's 2015 codification of PoC, but NATO itself would build on its experience in Kosovo in Afghanistan. In the wake of civilian casualty incidents from 2006 to 2008, which the Alliance feared would damage the mission's legitimacy and effectiveness, the International Security Assistance Force (ISAF) sought to cultivate positive relationships with NGOs active in Afghanistan, especially the International Committee of the Red Cross/Red Crescent (ICRC) and Center for Civilians in Conflict (CIVIC). Both of these NGOs engaged with ISAF at the combat and command levels, and ultimately both of them contributed to the establishment of non-binding guidelines on civilian protection in 2010.[17]

While this adaptive approach has produced promising results, this is not to suggest it has been without issues. From a practical perspective, KFOR's use of liaison officers improved relations with some NGOs, but it did not resolve all tensions between the Alliance and NGOs in Kosovo and introduced some new problems as well. The success of liaison officers in defusing tension between NATO and NGO personnel appeared to depend on the personalities of the interlocutors.[18] The discordant cultures of KFOR and the NGOs working in Kosovo created sources for tension. Where KFOR officials were comfortable giving instructions to NGOs to try to most efficiently distribute resources, NGO officials were just

[15] *Gheciu, 2011, pp. 101-102.*

[16] *Reinhardt 2000.*

[17] *Charlotte, Colli, and Reykers 2024, pp. 12-13.*

[18] *Gheciu, 2011, pp. 101-102.*

as comfortable telling KFOR officials they do not take orders from them.[19] Moreover, NATO's role in humanitarian relief and post-conflict reconstruction activities during or after conflicts in which the Alliance participated is seen by some NGOs and scholars as violating the neutrality at the heart of many of their missions.[20] The ICRC attempts to take a deliberately neutral stance to help secure access to areas and people most in need of assistance.[21] To this point, one NGO worker was quoted as not wanting to be seen working too closely as it would compromise their ability to carry out their work, reporting that a Serb villager told them, "Why should we trust you, if you were just bombing us and working with NATO?".[22]

In short, NATO's reactive, adaptive approach to emergent challenges has produced heartening results, but there are important limits to this approach, especially given the constraints of DZI. First, it cannot resolve all issues and incompatibilities the Alliance faces. Second, while some adaptations produce laudable results, they take time to do so. As difficult as it can be to summon the will to adapt to a problem before its effects are directly felt, this is precisely what the Alliance must do.

NATO and Ukraine—a public-private networking success story?

The Alliance has collaborated beyond its member states' borders and continues to do so in service of peace.[23] This extends both to partner nation governments and members of the defence industry. To this end, the provision of military aid by NATO member state governments in the war in Ukraine is especially instructive. Specifically, as Ukraine faced invasion, governments and firms alike put aside other concerns to collaborate in providing materiel to Ukraine.

Industry figures took note of the change the war in Ukraine brought, raising the issue during 2023's NATO-Industry Forum (NIF23). During NIF23, participants noted governments, seeking to reinforce Ukraine's efforts to repulse an invasion from a foreign aggressor, cut corners on procurements to facilitate deliveries on their behalf. One session observed many of the traditional barriers to collaboration between firms were overcome quickly in the wake of Russia's invasion. Specifically, firms ceased to compete against each other in some circumstances, instead partnering together to respond to pressing needs in the wake of the invasion.[24] To this end, NIF23 concluded that members needed to adopt open architectures in service of interoperability and to facilitate defense industry collaboration. While a crisis with a clear instigator may help encourage collaborative efforts for the reason of right alone, eschewing proprietary architectures can facilitate large, so-called "prime" members of the industry to collaborate with small to medium-sized enterprises (SMEs). These SMEs can help primes meet long-term goals by providing R&D, new technologies, and novel perspectives, while the primes can help these SMEs scale up their efforts.[27] NIF23 participants also noted relaxed procurement restrictions could facilitate better coordination between the Alliance and the defense industry.[27] Both the EU and US have trade restrictions aimed at preventing arms, materiel, and sensitive technology from falling into the hands of adversaries.[28] However, these restrictions were also cited by forum participants as obstacles to providing aid to Ukraine.[29]

Once again, a crisis pushes actors in NATO's orbit to adapt and they do so, as potential sources of friction gave way to a desire to help. As NIF23 demonstrates, the Alliance seeks to adapt in the face of new developments by incorporating non-state actors. Despite this, NIF23 also bears witness to the limitations of NATO's approach. As helpful as immediate adaptations were, the forum's participants noted that further adaptations are necessary to take full advantage of what the actors (those present at the forum) can bring to the table.

[19] *Minear, van Baarda, and Sommers 2000, p. 59.*
[20] *Gheciu, 2011, pp. 101*
[21] *Rieffer-Flanagan 2009, pp. 894-896.*
[22] *Minear, van Baarda, and Sommers 2000, pp. 51-52.*
[23] *"Strategic Concept" 2022.*
[24] *"NATO Industry Forum 2023 Report" 2024, p. 26.*
[25] *Temple-Reston 2022.*
[26] *"NATO Industry Forum 2023 Report" 2024, pp. 6, 14*
[27] *Ibid. p. 26.*
[28] *Viksnins 2024; Sabatino 2024.*
[29] *"NATO Industry Forum 2023 Report" 2024.*

MDOs IN NATO

The Allied Reaction Force (ARF) conducted exercise STEADFAST DART from January to February 2025, involving approximately 10,000 troops from nine NATO members moving thousands of kilometers.[30] This exercise demonstrated the readiness of ARF—a replacement for the NATO Response Force[31]—to rapidly deploy to the Alliance's eastern flank, carry out, and sustain complex operations in accordance with NATO's new Force Model. The Alliance's previous Force Model aimed to make 40,000 troops available in fewer than 15 days, but the new model (completed in 2023) intended to make more than 100,000 troops available with up to 10 days' notice.[32]

More importantly, Supreme Headquarters Allied Powers Europe (SHAPE) described the exercise as demonstrating operational capability "across all domains," noting the inclusion of "cyber and electronic warfare elements".[33] The inclusion of these non-traditional domains was as intentional as the exercise's speed. ARF is designed to serve as a means of delivering MDOs, as per 2023's Vilnius Summit Communiqué.[34]

[30] "STEADFAST DART – STDT25 Factsheet" 2025.
[31] "Allied Reaction Force (ARF)" 2025.
[32] "New NATO Force Model" 2022.
[33] "NATO's Allied Reaction Force Embarks on Eastern Europe's Largest Military Training Exercise in 2025" 2025; SHAPE's publication did not discuss the domain of space.
[34] Vilnius Summit Communiqué 2023.

Joint operations are nothing new, but MDOs represent a more holistic approach to incorporating and coordinating actions across branches, states, organizations, and firms as a means of addressing ongoing and emergent security challenges to the Alliance and beyond it. NATO's MDO concept describes "the orchestration of military activities, across all domains and environments, synchronized with non-military activities, to enable the Alliance to deliver converging effects at the speed of relevance".[35] The Alliance recognizes five domains as part of its this concept—land, maritime, air, space, and cyberspace. This reflects both an expansion beyond traditional warfighting domains as well as an explicit inclusion of non-military elements. Some of these transitions are easier than others. For instance, non-military elements have already been incorporated formally into operations, leveraging the "Comprehensive Approach" or by integrating "contributing non-military actions".[36] On the other hand, space and (especially) cyberspace are less consistently recognized as conflictual domains (Ibid. p. 3) but represent opportunities to expand this pattern of incorporation, as private actors' "capabilities often surpass those of the military" in these domains (Harig 2024, p. 1). Expansion beyond the purely military joint operations concept reflects two concerns. First, incorporating non-military assets brings additional, potentially decisive resources to bear. Non-military actors often possess useful expertise or insight regarding challenges faced by the Alliance. Leveraging this knowledge as well as the innovation produced outside the military requires incorporating these actors (Ibid.). Second, these non-military assets are vulnerable to the ravages of conflict. Private sector actors are often targeted by way of interrupting or destroying essential infrastructure[37] or by seeking to undermine the legitimacy of governing institutions in the eyes of those actors[38]

While NATO's MDO concept is distinct, it bears resemblance to the US Army's concept, laid out in 2018.[39] In particular, both MDO concepts emphasize neutralizing A2/AD defenses and other elements of layered standoff and place substantial emphasis on preventing separation between partners in, as the Army Concept describes "time, space, and function".[40]

[35] *"Multi-Domain Operations: Enabling NATO to Out-pace and Out-think its Adversaries" 2022.*
[36] *Dekker, Gubbels, and Kalloniatis 2025, p. 10.*
[37] *Machmeyer 2021, pp. 74-78; Slayton 2017, p. 91.*
[38] *Prier 2017*
[39] *Dekker, Gubbels, and Kalloniatis 2025, p. 2*
[40] *Ibid; "US Army Multidomain Operations 2028" 2018 p. iii.*

WHAT OF DZI?

For NATO's MDO concept, the "speed of relevance" is instantaneous. Russia's 2014 invasion of Ukraine's Donbas region and annexation of Crimea serve as a useful object lesson here, as Russia leveraged a combination of conventional, hybrid, and cyber warfare to rapidly achieve its objectives, deploying A2/AD capabilities to the seized regions.[41] The multiple leveraged domains, the speed at which Russian elements were able to pursue and achieve their objectives, and the degree to which the action caught Allies off guard all demonstrate the necessity of having as many potential instruments of power available to respond in concert as soon as a conflict begins.

Responding to such challenges in a timely manner requires DZI—the seamless integration of all available instruments working in concert before a conflict or crisis emerges. While military instruments of power can serve as a connective "hub," DZI also requires proactively cultivating similar connections to "partner nations, relevant international organisations such as the UN or EU, non-governmental organisations, civilian actors and industry".[42] These connections not only provide essential support in achieving an operation's objectives, but also provide the means of cultivating and bolstering resilience, facilitating military and civilian actors alike to withstand crises and respond in a synchronized and effective manner.[43]

DZI is also necessary given the five core tenets Andrea Gilli, Mauro Gilli and Gorana Grgić ascribe to MDOs: integration, synchronization, information and decision superiority, agility and adaptability, and cross-domain advantages.[44] By its definition, DZI addresses the first two tenets, but MDOs also require leveraging cutting-edge intelligence, surveillance, and reconnaissance (ISR) capabilities in part to retain the ability to immediately react effectively as the situation changes, up to and including shifting forces as necessary across large distances. Finally, MDOs require exploiting relative advantages, synchronizing interoperable assets across services to disintegrate elements of a layered standoff. However, this arrangement also brings potential problems, especially given the Alliance's pattern of adaptation.

The degree of frictionless integration across domains, capabilities, and actors NATO's MDO concept requires leaves Gilli, Gilli, and Grgić pessimistic regarding the Alliance's ability to achieve DZI. They list, among other things, issues related to C2, interoperability, information and intelligence sharing, Alliance member investment, and the state of NATO's cyber infrastructure amid potential roadblocks to the Alliance's ambitions.[45] While NATO has dedicated substantial effort to resolve these problems,[46] they possess the potential to constrain application of its MDO concept.

[41] *Quinn 2023, p. 17.*

[42] *NATO Warfighting Capstone Concept 2021, p. 21.*

[43] *Ibid.; "VII. Resilience."*

[44] *Gilli, Gilli, and Grgić 2025, pp. 75-76*

[45] *Ibid. pp. 78-85*

[46] *NATO STO Research Task Group SAS-143 2024; "NATO's Allied Reaction Force Embarks on Eastern Europe's Largest Military Training Exercise in 2025" 2025; "Hague Summit Declaration" 2025; "Joint Intelligence, Surveillance and Reconnaissance" 2025.*

The Alliance's history demonstrates a remarkable ability to respond to new challenges, taking on the advice, guidance, and experience-informed lessons of member states, other IOs, NGOs, and others. As successful as the Alliance's efforts have been to leverage this connective adaptivity, responding to crises as they come is no longer sufficient. Just as the Alliance has reinforced itself militarily, it must also reinforce its connections to and across governments, partner industries, and the private sector as a whole.

AREA 1:
MAKING THE MOST OF FNC

The Alliance's extant contingencies in the event of a crisis or conflict give reason for optimism. In 2016, the Warsaw Summit saw the creation of the Alliance's Enhanced Forward Presence forces (eFP), deployed along the Alliance's eastern flank to deter Russian aggression.[47] The eFPs are joined by both the Tailored Forward Presence in the southeast[48] as well as ARF.[49] These are not the only forces designed to respond rapidly to a crisis, though.

Indeed, some member states, under the auspices of the FNC (which also pertains to eFPs)[50] have been cultivating rapid response capabilities outside of the eFPs and ARF. For instance, 1GNC is in the process of transforming into an MDO-capable force able to neutralize the means of establishing a layered standoff.[51]

Brendan Flynn describes forces like the 1GNC as "interstitial" as they exist "at the interstices between the national level and multilateral organizations." In doing so, they offer a means to circumvent problems of, for instance, insufficient resources at the national level and deadlock at the international organizational level without acting as a rival to either.[52] Forces such as these may be able to act before an Alliance-wide consensus on a crisis coheres.

Another such force is the JEF, formed in response to Russia's invasion of the Donbas region and annexation of Crimea in 2014.[53] Despite the United Kingdom's predominant role in shaping the JEF, it incorporates several countries in the High North, North Atlantic, and Baltic Sea regions – including then partners Finland and Sweden in 2017.[54] Moreover, the rapidity with which the JEF could react is a part of its ostensible utility—as Royal Marines Brigadier Matt Jackson put it in 2019, "the JEF can act while NATO is thinking".[55] Finally, Standing Joint Force Headquarters appears dedicated to employing JEF across domains,[56] suggesting a possible fit with NATO's MDO concept.

Collaboration between the JEF and 1GNC may become necessary as neither possess sufficient mass to respond during a crisis. Marlow and Blythe note that, should the 1GNC be deployed at a conflict's outset, it would likely be at a numerical disadvantage with limited support from air and maritime elements.[57] Where the JEF is concerned, despite claims to readiness, NATO reacted more

[47] *Luik and Praks 2017.*
[48] *"NATO's military presence in the east of the Alliance" 2025.*
[49] *"Allied Reaction Force (ARF)" 2025.*
[50] *"NATO's military presence in the east of the Alliance" 2025.*
[51] *Marlow and Blythe 2022, pp. 17, 22-26.*
[52]*Flynn 2023, pp. 313-315.*
[53] *Ibid. pp. 319, 325-326*
[54] *JEF Vision 2023; Bond 2024*
[55] *Eckstein 2019.*
[56] *Peach and Boyd 2023*
[57] *Marlow and Blythe 2022, pp. 23-25.*

quickly to the sabotage of Balticonnector in October 2023,[58] deploying troops before the JEF was able to act. Collaborating may benefit both forces' utility in future crises.

Still, there are concerns Germany's "Culture of Restraint" may prevent it from responding in a timely fashion to material threats, especially given the additional weight the FNC gives to its "Framework Nations".[59] Sean Monaghan and Ed Arnold note that, for as flexible in its portfolio of active participants can be in a given operation, the JEF represents what they see as an eminently useful example of best practices for the concept, displaying (among other things) clarity of purpose, consistent communication of such, and leadership on the part of its Framework Nation.[60]

Moreover, German forces are constitutionally constrained to conducting operations "under the aegis of collective security and defense organizations." As the JEF seeks to act an instrument of ad hoc "coalitions of the willing" to respond to emergent crises, Germany is constitutionally prevented from participating in its missions.[61] For this reason, German Vice Adm. Jan Christian Kaack went as far as calling the force a "distraction" from NATO efforts in the Baltic region. [62]

[58] *Schmitz 2024.*

[59] *Saxi 2017, pp. 185-186.*

[60] *Monaghan and Arnold 2022, pp. 7-9.*

[61] *Puglierin 2021.*

[62] *Bond 2024.*

AREA 2: CYBERSPACE AS INFRASTRUCTURE

Integration with cyberspace is already paramount in every contemporary operation and promises to continue to be so.[63] This makes the challenges associated with the domain of cyberspace ones that must be resolved if Alliance MDOs are to achieve DZI.

Cyberattacks against Ukraine serve as important reminders of this fact. The NotPetya attack launched by the Russian Glavnoye Razvedyvatelnoye Upravlenie-affiliated group Sandworm decreased the Ukrainian GDP by 0.5% in 2017.[64] Still, there are ample reasons for optimism regarding the Alliance's task. Namely, the nature of cyberattacks make defense more feasible than some commentators suggest.[65] High-profile cyberattacks are often costlier than effective defenses are[66] and do not account for the attacker's own assets being damaged by such attacks, as was the case with NotPetya.[67] Additionally, Maschemeyer posits attackers must select from at most two of operational speed, the intensity of an attack's effects (especially if they are intended to be kinetic), and operational control.[68]

Regardless, the Alliance faces a daunting task in ensuring adequate cybersecurity of both military capabilities and infrastructure.[69] While networked controls for power plants and grids have justifiably grabbed headlines given the attacks on Ukrainian

[63] *Sherwood 2025.*
[64] *Maschemeyer 2021, pp. 79-82.*
[65] *Lin 2020.*
[66] *Slayton 2017.*
[67] *Maschemeyer 2021, pp. 79-82.*
[68] *Ibid. pp. 63-65.*
[69] *Gilli, Gilli, and Grgić 2025 pp. 80-81.*

electrical infrastructure,[70] they are far from the only potential targets. For example, an alleged attack on a Florida water treatment plant in 2021 was ostensibly to introduce dangerous levels of sodium hydroxide to the water supply.[71] The attack confirmed the concerns some cybersecurity experts had been voicing about water and sewage treatment infrastructure, representing a tantalizing target for bad actors and is perilously vulnerable to such attacks. One consultant also highlighted the fact that introducing such dangerous levels of sodium hydroxide was even possible using the system in the first place, describing the issue as: "control system 101 territory"[72]. Investing in computer infrastructure and putting effective practices into place at the local level can help mitigate these sorts of issues.

Shoring up vulnerable infrastructure is not merely a matter of applying best practices, though. There is also the issue of discovering new vulnerabilities and mitigating them, ideally before they are exploited. In the wake of many high-profile cyberattacks, the vulnerabilities are often identified and patched relatively quickly,[73] facilitating ongoing adaptations in defending against such attacks.[74] This adaptation is insufficient for a number of reasons, however.

First, high-profile cyberattacks tend to inspire copycats, especially when the attack is innovative. Bellovin, Landau, and Lin argue that conducting a sophisticated cyberattack presents a substantial and predictable proliferation risk.[75] For example, the discovery of the Stuxnet attack on Iranian nuclear infrastructure appears to have inspired several similar attacks over the years.[76]

Second, the efforts to patch out vulnerabilities, even in the wake of high-profile attacks, are not always foolproof. Stuxnet is once again a perfect

[70] *Ilevičius 2022; Machmeyer 2021, pp. 77-79, 84.*
[71] *Bergal 2021.*
[72] *Kardon 2023.*
[73] *Chen 2014, p. 9.*
[74] *Lin 2020; Lyngaas 2021.*
[75] *Bellovin, Landau, and Lin 2019, pp. 279-282.*
[76] *Ilevičius 2022; Machmeyer 2021, pp. 77-79, 84.*

example, with SafeBreach Labs discovering new zero-day (heretofore undiscovered and therefore unprotected) vulnerabilities related to the Stuxnet attack in 2020, a decade after its launch.[77] In other words, copycats could take advantage of similar vulnerabilities well after its discovery, further encouraging the development of copycat cyberweapons.

Mitigating critical system vulnerabilities can be done by both member states and private actors. The latter has been busy in this respect. The Cyber Defense Assistance Collaboration's (CDAC) work in Ukraine at the start of Russia's invasion serves as a potential model for private sector action.[78] CDAC solicited cybersecurity firms for assistance in sweeping them to look for malign actors' intrusions. Cybersecurity firm Mandiant volunteered to perform such a sweep for Naftogaz, a Ukrainian state-owned oil and gas firm. Even more encouraging is the speed at which CDAC was able to respond. As Greg Rattray, CDAC's Executive Director, stated, recounting his efforts in the war's early days: "I think the war started on a Thursday and I started making calls on the Monday".[79]

This is important for a number of reasons. First, this demonstrates an independent organization was quickly able to secure help from private sector cybersecurity experts for a vulnerable state firm. Second, this moment of extraordinary collaboration, where conflicting interests gave way to the desire to help, was made possible by the nature of the crisis itself. Just as was the case regarding government procurement rules and industry competition in the wake of the war in Ukraine's onset, so too was the profit motive superseded by the desire of individuals at the firm to help on behalf of a country subject to a clear instance of aggression.[80]

This is not to say the private sector can be tasked with addressing the problem in its entirety. Microsoft is a useful object lesson here; the firm contributed to Ukraine's successful cyber resilience, as did many others.[81] Microsoft has also earned plaudits both for spearheading 2018's Cybersecurity Tech Accord—an agreement signed by 34 tech firms "agreeing to defend all customers everywhere from malicious attacks by cybercriminal enterprises and nation-states"[82]—and for seeking to shape best practices regarding both information and communications technology (ICT) firms and nation-states alike.[83] On the other hand, Microsoft's website creation and document hosting software SharePoint was compromised in July of 2025 and exploited by several groups affiliated with the Chinese government.[84] More than 400 organizations had their data compromised,[85] including the National Institutes of Health and the United States Departments of Health and Human Services and Homeland Security.[86]

Alliance member state actors can help by more effectively disseminating insights their militaries and intelligence communities have learned to private sector actors. For example, U.S. Cyber Command's "UNDER ADVISEMENT"[87] seeks to facilitate information sharing between the US government and private sector partners. This can be quite useful, as Cyber Command and the National Security Agency (NSA) "often have intelligence about cyberattacks before or while they are happening".[88] For instance, if Cyber Command had discovered one of the zero-day exploits used in the attack on SharePoint,[89] its damage could have been more effectively mitigated.

The obvious issue here lies with a major appeal of cyberweapons—their secrecy.[90] Alliance members would almost certainly wish to avoid suggesting culpability in cyberattacks for a variety of reasons. First, leaders may be reticent to admit culpability

[77] *Culafi, 2020.*
[78] *Temple-Reston 2022.*
[79] *Ibid.*
[80] *Ibid.*
[81] *Kramer, Dailey, and Brodfuehrer 2024, pp. 9-10.*
[82] *Maurer 2018.*
[83] *Charney 2016.*
[84] *Microsoft Threat Intelligence 2025.*
[85] *Whittaker 2025.*
[86] *Brennan et al 2025.*
[87] *"Private Sector Partnerships" 2025.*
[88] *Temple-Raston 2022.*
[89] *Whittaker 2025.*
[90] *Maschmeyer 2021, p. 54.*

in a cyberattack for fear that doing so could lead to reprisals or escalation.[91] Second, revealing zero-day exploits means forgoing the use of such vulnerabilities in future attacks and the sacrifice of the substantial time and effort associated with covertly discovering them and developing the means to exploit them. [92]

Unfortunately, experience suggests information sharing is often constrained, even between government agencies. The information sharing environment often privileges the control of information held by military and intelligence actors over its dissemination to agencies, even within the military and intelligence communities.[93] Worse, a discovery of vulnerability does not necessarily mean it can no longer be used. Processes such as code refactoring render vulnerabilities unusable or resuscitate so-called “dead” ones (2017, pp. 51-52).[94] This means even if the information is shared, it might be misleading if the listener lacks the necessary expertise or context.

[91] Schneider 2016.
[92] Maschmeyer 2021, pp. 65-67.
[94] Albon, Lillian, and Andy Bogart 2017, pp. 51-52; by dead, the authors mean discovered or “publicly known” instead of “alive” or “publicly unknown.”

AREA 3: CONCEPTUALIZING AND OPERATIONALIZING CONFLICT IN THE FINAL FRONTIER

Synchronizing operations across domains will inevitably involve space. While the Alliance does not seek to become an “autonomous actor” according to its Overarching Space Policy,[95] it has begun coordinating internally and externally to ensure the interoperability of member capabilities. One manifestation of this is the Alliance Persistent Surveillance from Space (APSS).

APSS represents a promising step forward into the final frontier.[96] The project confirms the Alliance’s dedication to leveraging both the capabilities of its member states and those of private firms to create and coordinate space-based ISR capabilities. In 2024, NATO signed a contract with satellite imagery firm Planet Labs to create “Aquila,” intended to serve as a “virtual constellation” of space-based ISR assets held by Alliance members.[97] This aligns with the Alliance’s Commercial Space Strategy, in which NATO seeks to collaborate with and leverage commercial interests to not only ensure the availability of services, but to meet the Alliance’s “operational and defense planning requirements”.[98] This is complemented by the launch of NORTHLINK in October of 2024, a project aiming to provide “secure, resilient and reliable multinational Arctic satellite communications capability”.[99]

The Alliance is also exploring the ability to add to its space-based assets rapidly, should circumstances determine such a need.[100] STARLIFT, launched the same month as NORTHLINK, aims to develop the capability to either launch new assets quickly, “manoeuvre a pre-positioned spare spacecraft or buy data from commercial partners during crisis or conflict”.[101] These sorts of investments ahead of time can help provide essential capabilities in the event of the outbreak of hostilities.

However, an adversary’s space-based ISR capabilities can give them a “nearly impenetrable” early warning system, substantively complicating efforts to disintegrate and destroy elements of A2/AD.[102] If the Alliance is to be tasked with doing so, it would need to leverage offensive capabilities among members to compromise space-based ISR capabilities.

Given the state of Alliance members’ space-based offensive capabilities, this is quite a tall task. Specifically, space is not thought of as a domain in which warfighting takes place due to the substantial contributions private-sector firms make to the US and other states interested in the domain.[103] A contributing factor may be a preference to maintain outer space as a domain free from warfighting. Indeed, in 2022 the US voluntarily committed to

[95] *“NATO’s Overarching Space Policy” 2025.*

[96] *“Alliance Persistent Surveillance from Space” 2023.*

[97] *Hadley 2024.*

[98] *“NATO Commercial Space Policy” 2024.*

[99] *“NATO launches five new multinational cooperation initiatives that enhance deterrence and defence” 2024.*

[100] *“NATO’s approach to space” 2025.*

[101] *“NATO launches five new multinational cooperation initiatives that enhance deterrence and defence” 2024.*

[102] *Vershinin 2020, p. 18.*

[103] *Galbreath and Reeves 2025, pp. 14-17.*

not test direct ascent anti-satellite (ASAT) missiles, with several other countries following suit.[104] Yet, it may be necessary to consider the domain as a host to warfighting.

Just as the APSS saw Luxembourg take on increased responsibility in the domain,[105] the United States appears prepared to contribute space-oriented warfighting capabilities with its relatively novel Space Force signaling increasing enthusiasm for deploying ASAT systems,[106] but problems exist here as well. First, Space Force still needs to develop and communicate a warfighting concept.[107] Second, the United States' systems that can be employed as kinetic ASAT weapons are both expensive and not high acquisition priorities.[108]

While both Russia and China are investing in kinetic ASAT weapons systems, and there are certainly those who advocate Alliance members do likewise (Galbreath and Reeves 2025, p. 15), others argue such systems would do more harm than good. For instance, some are concerned the destruction of a single satellite could in turn disrupt or destroy nearby satellites, such that even targeted satellite destruction could "render many areas in near-Earth space highly contaminated and unusable" (Czajkowski 2024, 184). The potential to impact non-target systems and produce substantial collateral damage is such that Leet Wood has argued kinetic ASAT weapons should be deemed Weapons of Mass Destruction (2021). This would create an international legal basis for eliminating such weapons, given the terms of the Outer Space Treaty (1967), but this is no guarantee they will be removed.

As dangerous as ASATs may be—both to their targets and to the free exercise of space generally[109]—this does not preclude the use of other systems that might be more discriminate in their effects. Electronic warfare, cyberattacks, and some directed energy weapons (DEWs) can be designed and employed in such a way they do not produce the collateral damage and unintended consequences of kinetic ASATs.[110] Additionally, "offensive countermeasures" (cyberweapons, electronic warfare, or lasers intended to "dazzle" satellites) can be effective in disrupting satellite operation without contributing as dramatically to escalation in outer space as destroying a satellite with a missile.[111]

[104] *Townsend 2024, p. 5.*
[105] *Wolfe 2024.*
[106] *Waterman 2025.*
[107] *Galbreath and Reeves 2025, pp. 4-5.*
[108] *Vershinin 2020, p. 14.*
[109] *Czajkowski 2024; Wood 2021.*
[110] *Wood 2021, pp. 70-71.*
[111] *Czajkowski 2024, p. 185.*

RECOMMENDATIONS

The first recommendation is that the Alliance should define relationships within and between Framework Nation-led multinational forces. The FNC itself provides a potential path forward in this regard. Germany's Basic Law prevents the Bundeswehr from participating in a "coalition of the willing" mission outside a UN, EU, or NATO framework. While some have argued this constraint should be abandoned given contemporary security concerns and the increasingly ad hoc manner in which multinational operations' coalitions are constructed, it nevertheless remains a major stumbling impediment to Germany's participation in such coalitions.[113] Still, the FNC remains a NATO concept. This is significant, as deployment in service of an ostensible collective security organization—or at least one that could be argued to be so—was used to justify Germany's participation in the EU's anti-ISIS mission.[114] This points to additional clarification and negotiation as the solution.

The United Kingdom and Germany can help assuage each other's concerns. Germany can provide clarity regarding the circumstances 1GNC would be deployed and all the moving political parts involved, including parliamentary approval necessary for action.[115] The corps is ostensibly designed to respond rapidly in a crisis[116] and was subject to substantial negotiations on the part of its participant nations from its founding.[117] If Germany can be clear regarding its own response, then the United Kingdom should be willing to respond in kind.

The United Kingdom's response will need to be tailored to the strictures of the Basic Law. One possibility could be a discussion regarding which states would constitute a "coalition of the willing" in the event of a given hypothetical crisis. Agreement ahead of time regarding the hows and whys could prevent circumstances such as October 2023's crisis. First, it would streamline the process of the JEF's deployment, potentially preventing a repeat of the force that was unable to arrive until after a force under the Alliance's banner did.[118] Second, a formal agreement regarding who would participate under what circumstances could facilitate German collaboration with a JEF mission. This would circumvent concerns regarding forming "coalitions of the willing" and provide collective security-oriented auspices for German participation, similar to that which allowed German participation in EU anti-ISIS operations.[119]

If this goes well, it could serve as a potential framework to resolve similar issues as other members work to apply the FNC. For example, Italy's application of the FNC could present similar issues as its application lags both the United Kingdom and Germany, especially in terms of the framework nation's visible leadership and

[113] *Bond 2024.*
[114] *Puglierin 2021.*
[115] *Ibid.*
[116] *Marlow and Blythe 2022.*
[117] *Fleck 2000, pp. 163, 171-175.*
[118] *Bond 2024.*
[119] *Puglierin 2021*

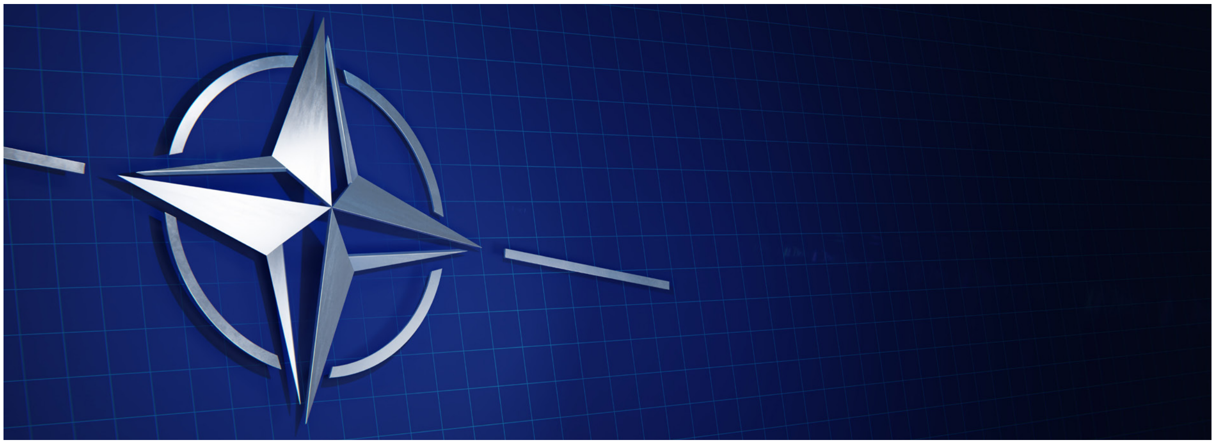
consistent activity among participants.[120] Italy's government ought to take pains to ensure its ability to collaborate with as many members as possible. If the apparent incompatibilities between Germany and JEF are resolved, then this may be relatively simple.

The second recommendation is that the Alliance should cultivate opportunities to disseminate new discoveries and facilitate private-public collaboration to shore up Allies' defenses in cyberspace. CDAC demonstrates, to some degree, that cybersecurity experts are amenable to contribute their expertise in service of defending vulnerable public infrastructure. Whether this is possible at scale remains an open question. Even if governments or their agencies are willing to disseminate what they know on existing or newly discovered vulnerabilities, the information may not be immediately useful.

The best path forward may be to take pains to cultivate networks among and across Alliance members to span the public and private divide. Such networks are hardly novel, even for the Alliance,[121] as governments often rely on non-governmental actors to solve problems not well-suited to hierarchical relationships due to complexity or the availability of resources.[122] Cultivating networks of cybersecurity experts from the private sector and pertinent officials from the Alliance's governments and their agencies could help facilitate more effective means to prevent cyberattacks and mitigate the effects of successful ones.

Public policy networks have produced noteworthy cooperation across potentially thorny barriers to such. In particular, research suggests that productive networks can be formed by groups of governmental officials and private-sector experts, especially where these different groups can provide unique resources.[123] Moreover, information exchange appears to be more likely within networks where actors have different organizational backgrounds, the rationale being that information coming from different parts of a network would likely be more useful for a given actor compared to information coming from a more similar actor. Furthermore, successes in counterterrorism networks suggest that information can be disseminated among officials and experts while respecting pertinent legal prohibitions regarding disclosure.

While stable involvement across the public-private divide often requires mutually determined relationships,[126] NATO's experience cultivating emergent networks gives reason for optimism. In particular, Federated Mission Networking (FMN) not only supports interoperability in missions but can create and cultivate networks across diverse groups of actors in service of NATO operations.[127] This experience in bringing together different



[120] Monaghan and Arnold 2022, p. 7.
[121] "Day Zero Integration" 2024.
[122] O'Toole 1997.
[123] Siciliano, Wang, and Medina 2021, pp. 71-72.
[124] Schrama 2019, pp. 570-71.
[125] Bayer 2010, p. 19.
[126] Ysa 2007, pp. 39-40.
[127] "Federated Mission Networking" 2025.

actors as well as materiel and non-materiel resources in service of a broader mission should help facilitate collaboration in both crisis and non-crisis scenarios.

Empirical research suggests cultivating such connections is eminently feasible. Even when networks are explicitly cultivated by way of governmental intervention, this intervention motivates coordination within the networks in question.[128] Moreover, this effect is especially prominent where organizations did not already share a tie with one another or did not belong to a group akin to the network already.[129] Such a network could encourage new contributors to the Alliance's cybersecurity and potential beneficiaries to seek aid.

CDAC's intervention on behalf of Ukrainian infrastructure at the outset of Russia's invasion[130] provides a clear and potentially instructive example of how such a network might be useful in the event of hostilities against an Alliance member. This is not the only way such a network could aid DZI, though. The diffusion of information regarding newly discovered threats and best practices, especially to agencies without the resources to invest heavily in cybersecurity, could prevent the exploitation of potentially vulnerable infrastructure and safeguard information and assets of the Alliance's populations.

The third recommendation is that the Alliance should consider encouraging members to develop and deploy new weapon systems to this new battlefield. The development of new weapon systems by potential adversaries[131] means the Alliance will need to prepare contingencies in order to maintain its coordinated space-based ISR capabilities, to say nothing of responding to adversaries' capabilities in a future conflict.

Before doing so, the Alliance must clarify its position regarding warfare in space. While some members voice frustration regarding the impact of 1967's Outer Space Treaty on space's image as something of a realm free from militarization,[132] the treaty's language[133] (1967) is nevertheless reflected in the Alliance's Overarching Policy regarding space.[134] Given the potentially devastating unintended consequences of kinetic, destructive ASAT systems, trepidation at deploying such systems is, at minimum, understandable (Wood 2021, Czajkowski 2024).

This does not preclude the use of weapons systems either in space or against assets therein. Free access and exploration are also concepts applied to open water,[135] yet warfare persists in the maritime domain. Obviously, this comparison is not without complications—for one, the Outer Space Treaty stipulates space is not subject to claims of sovereignty, whereas the UN Convention on the Law of the Sea allows sovereignty[136] to manifest itself upon the waves in a number of ways.[137] Nevertheless, such clarification would help reduce friction among members, partners, and other entities by reducing uncertainty.

It might also help prioritize the development of weapons without the collateral effects of kinetic ASAT weapons if the Alliance finds it appropriate to forgo their use. While the United States appears prepared to leverage such weapons, advocates appear to do so out of concern for developing and deploying the means of effective warfighting in space.[138] Moreover, these non-destructive or non-kinetic systems are anything but novel—some countermeasures (e.g. electronic countermeasures to "jam" or "dazzle" satellites) are found in a Cold War-era report to the US Congress on ASAT weapons.[139]

[128] *Scott 2016.*
[129] *Ibid.*
[130] *Temple-Reston 2022.*
[131] *Galbreath and Reeves 2025, p. 15; Waterman 2025; Czajkowski 2024.*
[132] *Galbreath and Reeves 2025, pp. 15, 21.*
[133] *"Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies." 1967.*
[134] *"NATO's Overarching Space Policy" 2025.*
[135] *UN General Assembly 1982.*
[136] *"Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies." 1967.*
[137] *UN General Assembly 1982.*
[138] *Galbreath and Reeves 2025, pp. 17, 19.*
[139] *U.S. Congress 1985, pp. 4, 7-8.*

CONCLUSION

While chance's role in introducing friction makes foolproof contingencies impossible,[140] working to proactively reduce frictional barriers to effective operations can facilitate timely and effective response in a crisis. The Alliance's dizzying array of military and non-military assets and the myriad political interests and protocols to which each are subject makes integration and synchronization before a conflict's outset necessary. NATO's history has many examples of reactive—and effective—adaptation to emergent challenges, but doing so going forward regarding friction will render MDOs ineffectual. Instead, the Alliance must seize opportunities to address friction before it threatens effectiveness.

First, both 1GNC and the JEF promise to deliver substantial capabilities in response to a crisis or conflict and do so quickly, adding to the Alliance's ample capabilities to defend itself. However, tensions among Framework Nations—namely the UK and Germany—limit the efficacy of such forces by introducing barriers to their cooperation.

Second, cyberspace represents a material vulnerability for NATO, in terms of military and non-military cyber infrastructure in both the public and private spheres. Firms and government agencies may find themselves targeted by sophisticated cyberattacks, representing potentially devastating vulnerabilities for member state governments and their populations.

Finally, the Alliance has taken admirable steps toward clarifying its position regarding outer space and coordinating its collective capabilities within the domain, but its position remains unclear regarding warfighting within it. As essential as projects such as APSS are to coordinating ISR capabilities, the Alliance remains somewhat unclear regarding efforts to address potential adversaries in space. Further clarification regarding kinetic and non-kinetic space-based weapons will aid member-states to properly orient towards Allied objectives.

These and other potential sources of friction can be addressed if the Alliance leverages its impressive ability to bring disparate actors together. The FNC has already produced productive collaboration—doing so among its Framework Nations is hardly a stretch. The same can be said regarding bringing member state governmental officials, industrial representatives, and experts together—the Alliance already does this to great effect. Doing so with the express intent of facilitating Alliance-wide, bottom-up improvements in defending cyberspace merely builds on this practice. Finally, the Alliance has already made strides in clarifying its position regarding outer space and has seen Allies begin to take on specialized tasks regarding this domain. Questions remain, but answering them only requires that the Alliance continue to build on the work already in progress.

[140] *Clausewitz 1989, p. 120.*

REFERENCES

- Albon, Lillian, and Andy Bogart. 2017. Zero Days, Thousands of Nights: The Life and Times of Zero-Day Vulnerabilities and their Exploits. Santa Monica, CA: Rand Corporation. https://www.rand.org/pubs/research_reports/RR1751.html.

- Bayer, Michael D. 2010. The Blue Planet: Informal International Police Networks and National Intelligence. Washington, D.C.: National Intelligence Press.

- Bellovin, Steven M., Susan Landau, and Herbert Lin. 2019. "Limiting the Undesired Impact of Cyber Weapons: Technical Requirements and Policy Implications" In Bytes, Bombs, and Spies: The Strategic Dimensions of Offensive Cyber Operations, edited by Herbert Lin and Amy Zegart. (Washington, D.C.: Brookings Institute Press): 265-288.

- Bergal, Jenni. 2021. "Florida Hack Exposes Danger to Water System," Stateline, 10 March. https://stateline.org/2021/03/10/florida-hack-exposes-danger-to-water-systems/.

- Bond, Ian. 2024. "The Joint Expeditionary Force: Deterrent, Defender, or Distraction?" Carnegie India, December 6. https://carnegieendowment.org/research/2024/12/the-joint-expeditionary-force-deterrent-defender-or-distraction?lang=en&center=india.

- Brennan, Margaret, James LaPorta, Camilo Montoya-Galvez, Olivia Rinaldi. 2025. "DHS and HHS among federal agencies hacked in Microsoft Sharepoint breach," CBS News, 24 July. https://www.cbsnews.com/news/microsoft-sharepoint-breach-dhs-hhs/.

- Carlson, Randall E., and Ron Gurantz. 2022. "Clausewitz in Space: Friction in Space Strategy and Operations." Æther: A Journal of Strategic Airpower & Spacepower 1(3): 65-80. https://www.jstor.org/stable/48681611.

- Charlotte, Daphné, Francesca Colli, and Yf Reykers. 2024. "From policy to practice: How NATO joined forces with NGOs for the protection of civilians." Cooperation & Conflict: 1-28. https://doi.org/10.1177/00108367241288082.

- Charney, Scott. 2016. "Cybersecurity norms for nation-states and the global ICT industry." Microsoft On the Issues, June 23. https://blogs.microsoft.com/on-the-issues/2016/06/23/cybersecurity-norms-nation-states-global-ict-industry/.

- Chen, Thomas M. 2014. Cyberterrorism After Stuxnet. Carlisle Barracks, PA: Strategic Studies Institute, US Army War College.

- Clausewitz, Carl von. 1989. On War. Edited and translated by Michael Howard and Peter Paret. Princeton: Princeton University Press.

- Culafi, Alexander. 2020. “10 years after Stuxnet, new zero-days discovered,” TechTarget, 7 August. https://www.techtarget.com/searchsecurity/news/252487374/10-years-after-Stuxnet-new-zero-days-discovered.

- Czajkowski, Marek. 2024. “Anti-Satellite Weapons – Current Status,” Roczniki nauk społecznych 52(4): 183-201. https://doi.org/10.18290/rns2024.0043.

- Dekker, Ralph, Frank Gubbels, and Alex Kalloniatis. 2025. “From Concept to Capability: In the NATO’s C2 of Multi-Domain Operations - History, Evolution and Challenges,” NATO C2COE, 17 January. https://c2coe.org/download/from-concept-to-capability-in-the-natos-c2-of-multi-domain-operations-history-evolution-and-challenges/.

- Eckstein, Megan. 2019. “New U.K.-Led Maritime First Responder Force Takes to Sea at BALTOPS,” USNI News, 21 June. https://news.usni.org/2019/06/21/new-u-k-led-maritime-first-responder-force-takes-to-sea-at-baltops.

- Fleck, Dieter. 2000. “Legal Issues of Multinational Military Units Tasks and Missions, Stationing law, Command and Control,” International Law Studies 75(1): 161-178.

- Flynn, Brendan. 2023. “Knowing your CJEF from your JEF: Europe’s ‘Alphabet soup’ of Interstitial military cooperation-what relevance for cold war 2.0?” Defence Studies 23(2): 313-333. https://doi.org/10.1080/14702436.2022.2137495.

- Galbreath, Col Charles S. and Col Jennifer K. Reeves. 2025. “Ensuring a Spacepower Advantage in Prolonged Competition: Findings and Recommendations from the Space Endurance Workshop,” Mitchell Institute for Aerospace Studies, February. https://www.mitchellaerospacepower.org/ensuring-a-spacepower-advantage-in-prolonged-competition-findings-and-recommendations-from-the-space-endurance-workshop/.

- Gheciu, Alexandra. 2011. “Divided Partners: The Challenges of NATO-NGO Cooperation in Peacebuilding Operations,” Global Governance 17: 95-113.

- Gilli, Andrea, Mauro Gilli, and Gorana Grgić. 2025. “NATO, multi-domain operations and the future of the Atlantic Alliance,” Comparative Strategy 44(1): 73-91. https://doi.org/10.1080/01495933.2024.2445491.

- Hadley, Greg. 2024. “NATO Signs First Contract for Its Largest Space Program Ever,” Air and Space Forces Magazine, 19 August. https://www.airandspaceforces.com/nato-contract-satellite-imagery-space/.

- Harig, Christoph. 2024. “The Future of Civil-Military Cooperation in NATO,” Centre for Historical Analysis and Conflict Research, November. https://chacr.org.uk/2024/11/07/civil-military-cooperation-in-nato/.

- Ilevičius, Paulius. 2022. “Stuxnet explained — the worm that went nuclear” NordVPN, 10 March. https://nordvpn.com/blog/stuxnet-virus.

- Johnson, David E. 2018. “Shared Problems The Lessons of AirLand Battle and the 31 Initiatives for Multi-Domain Battle,” RAND Corporation, 13 September. https://www.rand.org/pubs/perspectives/PE301.html.

- Joint Expeditionary Force. 2023. The JEF Vision. https://www.government.se/contentassets/c7b847cc5b9f49fc8de64dd0006278f4/jef_vision.pdf.

- Kardon, Steve. 2023. “Florida Water Treatment Plant Hit With Cyber Attack,” Industrial Defender, 10 April. https://www.industrialdefender.com/blog/florida-water-treatment-plant-cyber-attack.

- Kramer, Franklin D., Ann M. Dailey, and Joslyn A. Brodfuehrer. 2024. “NATO multidomain operations: Near- and medium-term priority initiatives,” Atlantic Council, 21 February. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/nato-multidomain-operations/.

- Luik, Jüri, and Henrik Praks. 2017. Boosting the Deterrent Effect of Allied Enhanced Forward Presence. Eesti: International Centre for Defence and Security. https://icds.ee/wp-content/uploads/2017/ICDS_Policy_Paper_Boosting_the_Deterrent_Effect_of_Allied_eFP.pdf.

- Lin, Herbert. 2020. “Reflections on the SolarWinds Breach.” Lawfare, December 22. https://www.lawfareblog.com/reflections-solarwinds-breach.

- Lyngaas, Sean. 2021 “US warns hundreds of millions of devices at risk from newly revealed software vulnerability” CNN, 14 December. https://www.cnn.com/2021/12/13/politics/us-warning-software-vulnerability/index.html.

- Marlow, Andreas, and Wilson C. Blythe, Jr. 2022. “Multi-Domain Warfaighting in NATO: The 1 German-Netherlands Corps View,” Military Review 102(3): 47-57.

- Maschmeyer, Lennart. 2021. “The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations.” International Security 46(2): 51-90.

- Maurer, Tim. 2018. “Private Companies Take the Lead on Cyber Security,” War on the Rocks, 4 May. https://warontherocks.com/2018/05/private-companies-take-the-lead-on-cyber-security/.

- McCranie, Kevin D. 2021. Mahan, Corbett, and the Foundations of Naval Strategic Thought. Annapolis, MD: Naval Institute Press.

- Microsoft Threat Intelligence, 2025. “Disrupting active exploitation of on-premises SharePoint vulnerabilities,” Microsoft, 22 July. https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/.

- Minear, Larry, Ted van Baarda, and Marc Sommers. 2000. NATO and Humanitarian Action in the Kosovo Crisis. Occasional Paper #36. Providence, RI: Institute for International Studies, Brown University. https://ciaotest.cc.columbia.edu/wps/wibu/0015215/f_0015215_12845.pdf.

- Monaghan, Sean, and Ed Arnold. 2022. “Indispensable: NATO’s Framework Nations Concept beyond Madrid,” Center for Strategic & International Studies, 27 June. https://www.csis.org/analysis/indispensable-natos-framework-nations-concept-beyond-madrid.

- NATO STO Research Task Group SAS-143. 2024. “Agile Multi-Domain C2 of Socio-Technical Organizations in Complex Endeavors Operating in a Contested Cyberspace Environment,” NATO C2COE, February. https://c2coe.org/agile-multi-domain-c2-of-socio-technical-organizations-in-complex-endeavors-operating-in-a-contested-cyberspace-environment/.

- NATO Warfighting Capstone Concept. 2021. NATO Allied Command Transformation, 18 May. https://www.act.nato.int/wp-content/uploads/2023/06/NWCC-Glossy-18-MAY.pdf.

- O’Toole, Lawrence. 1997. “Treating Networks Seriously: Practical and Research-Based Agendas in Public Administration,” Public Administration Review 57(1): 45-52.

- Parshall, Jonathan B. and Anthony B. Tully. 2005. Shattered Sword: The Untold Story of Midway. Washington, D.C.: Potomac Books.

- Peach, Stuart, and Robbie Boyd. 2023. "Stretching the Joint Expeditionary Force: An Idea for Our Times," Royal United Services Institute, 8 September. https://www.rusi.org/explore-our-research/publications/commentary/stretching-joint-expeditionary-force-idea-our-times.

- Puglierin, Jana. 2021. "The Engine Room: Germany, the Unwilling Coalition Partner," Internationale Politik Quarterly, May 3. https://ip-quarterly.com/en/engine-room-germany-unwilling-coalition-partner.

- Prier, Jared. 2017. "Commanding the Trend: Social Media as Information Warfare." Strategic Studies Quarterly 11(4): 50-85, https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf.

- Quinn, Bryan J. 2023. "Sustaining Multidomain Operations: The Logistical Challenge Facing the Army's Operating Concept," Military Review 103(2): 128-138.

- Reinhardt, Klaus. 2000. "Commanding KFOR," NATO Review, 1 September. https://www.nato.int/docu/review/articles/2000/09/01/commanding-kfor/index.html.

- Rieffer-Flanagan, Barbara Ann. 2009. "Is Neutral Humanitarianism Dead? Red Cross Neutrality: Walking the Tightrope of Neutral Humanitarianism," Human Rights Quarterly 31(4): 888-915. https://www.jstor.org/stable/40389980.

- Sabatino, Esther. 2024. "Arms Supplies to Ukraine: Does the European Arms Export Control System Need Revision?" Stockholm International Peace Research Institute, May. https://www.sipri.org/publications/2024/eu-non-proliferation-and-disarmament-papers/arms-supplies-ukraine-does-european-arms-export-control-system-need-revision.

- Saxi, Håkon Lunde. 2017. "British and German initiatives for defence cooperation: the Joint Expeditionary Force and the Framework Nations Concept," Defence Studies 17(2): 171-197. https://doi.org/10.1080/14702436.2017.1307690.

- Schmitz, Rob. 2024. "Sabotage suspected after undersea cables damaged in the Baltic Sea," NPR, 20 November. https://www.npr.org/2024/11/20/nx-s1-5197701/underwater-telecom-cables-in-the-baltic-sea.

- Schrama, Reini. 2019. "Swift, brokered and broad-based information exchange: how network structure facilitates stakeholders monitoring EU policy implementation," Journal of Public Policy 39(4): 565-585. doi:10.1017/S0143814X1800017X.

- Scott, Tyler A. 2016. "Analyzing Policy Networks Using Valued Exponential Random Graph Models: Do Government-Sponsored Collaborative Groups Enhance Organizational Networks?" The Policy Studies Journal 44(2): 215-244.

- Sherwood, Dorothy. 2025. "Sweden Cyber Command and Air Forces Cyber align cyber Compatibility," Sixteenth Air Force (Air Forces Cyber), 7 March. https://www.16af.af.mil/Newsroom/Article-Display/Article/4112360/sweden-cyber-command-and-air-forces-cyber-align-cyber-compatibility/.

- Siciliano, Michael D., Weijie Wang, and Alejandra Medina. 2021. "Mechanisms of Network Formation in the Public Sector: A Systematic Review of the Literature," Perspectives on Public Management and Governance 4(1): 63–81. doi:10.1093/ppmgov/gvaa017/

- Slayton, Rebecca. 2017. "What Is the Cyber Offense-Defense Balance?: Conceptions, Causes, and Assessment," International Security 41(3): 72-109.

- Temple-Reston, Dina. 2022. “EXCLUSIVE: Rounding up a cyber posse for Ukraine,” The Record, 17 November. https://therecord.media/exclusive-rounding-up-a-cyber-posse-for-ukraine.

- Townsend, Brad. 2024. “Moving Beyond an ASAT Ban,” Æther: A Journal of Strategic Airpower & Spacepower 3(4): 5-16. https://www.jstor.org/stable/48809072.

- UN General Assembly. 1982. Convention on the Law of the Sea, 10 December. https://www.refworld.org/legal/agreements/unga/1982/en/40182.

- U.S. Congress. 1985. Anti-Satellite Weapons, Countermeasures, and Arms Control. Washington, D.C.: U.S. Government Printing Office.

- Viksnins, Krista. 2024. “US Bureaucracy is Blocking Arms for Ukraine,” Center for European Policy Analysis, 5 July. https://cepa.org/article/us-bureaucracy-is-blocking-arms-for-ukraine/.

- Vershinin, Alex. 2020. “The Challenge of Dis-Integrating A2/AD Zone: How Emerging Technologies Are Shifting the Balance Back to the Defense,” Joint Forces Quarterly 97(2): 13-19.

- Waterman, Shaun. 2025. “Space Force Focused on the Ground for Anti-Satellite Weapons,” Air and Space Forces Magazine, 3 April. https://www.airandspaceforces.com/space-force-ground-anti-satellite-weapons/.

- Whittaker, Zack. 2025. “Hackers exploiting SharePoint zero-day seen targeting government agencies,” TechCrunch, 23 July. https://techcrunch.com/2025/07/21/hackers-exploiting-sharepoint-zero-day-seen-targeting-government-agencies-say-researchers/.

- Wolfe, Frank. 2024. “NATO Surveys the Space Capabilities of Member Nations,” Via Satellite, 10 October. https://www.satellitetoday.com/government-military/2024/10/10/nato-surveys-the-space-capabilities-of-member-nations/.

- Wood, Leet W. 2021. “The Myth of Tactical Anti-Satellite Weapons: Redefining and Effectively Controlling,” Astropolitics 19(1-2): 62-75. https://doi.org/10.1080/14777622.2021.1996206.

- Ysa, Tamako. 2007. “Governance Forms in Urban Public-Private Partnerships,” International Public Management Journal 10(1): 35-57.

- “Alliance Persistent Surveillance from Space.” 2023. NATO February. https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230215-factsheet-apss.pdf.

- “Allied Reaction Force (ARF).” 2025. NATO, 16 April. https://www.nato.int/cps/en/natohq/topics_234091.htm.

- “Day Zero Integration.” 2024. NATO CMDR COE, 13 June. https://cmdrcoe.org/menu.php?m_id=27m_id=27&n_id=394&page=1.

- “Federated Mission Networking.” 2025. NATO Allied Command Transformation. https://www.act.nato.int/activities/federated-mission-networking/.

- “The Hague Summit Declaration.” 2025. NATO, 25 June. https://www.nato.int/cps/en/natohq/official_texts_236705.htm.

- “Joint Intelligence, Surveillance and Reconnaissance.” 2025. NATO, 30 July. https://www.nato.int/cps/en/natohq/topics_111830.htm.

- “Multi-Domain Operations in NATO.” 2023. NATO Allied Command Transformation, October 5. https://www.act.nato.int/article/mdo-in-nato-explained/.

- “Multi-Domain Operations: Enabling NATO to Out-pace and Out-think its Adversaries.” 2022. NATO Allied Command Transformation, July 29. https://www.act.nato.int/article/multi-domain-operations-enabling-nato-to-out-pace-and-out-think-its-adversaries/.

- “NATO Commercial Space Strategy.” 2025. NATO, 24 June. https://www.nato.int/cps/en/natohq/official_texts_236520.htm.

- “NATO Industry Forum 2023 Report.” 2024. NATO ACT. https://www.act.nato.int/wp-content/uploads/2024/05/20240514_NIF-glossy.pdf.

- “NATO launches five new multinational cooperation initiatives that enhance deterrence and defence.” 2024. NATO, 17 October. https://www.nato.int/cps/en/natohq/news_229664.htm?selectedLocale=en.

- “NATO’s Allied Reaction Force Embarks on Eastern Europe’s Largest Military Training Exercise in 2025.” 2025. Supreme Headquarters Allied Powers Europe, 3 February. https://shape.nato.int/steadfast-dart/media-centre/news/arf-embarks-on-eastern-europes-largest-military-drill.

- “NATO’s military presence in the east of the Alliance.” 2025. 6 June. https://www.nato.int/cps/en/natohq/topics_234091.htm.

- “NATO’s Overarching Space Policy.” 2025. NATO, 24 June. https://www.nato.int/cps/en/natohq/official_texts_190862.htm.

- “Private Sector Partnerships.” 2025. U.S. Cyber Command. https://www.cybercom.mil/Partnerships-and-Outreach/Private-Sector-Partnerships/.

- “VII. Resilience.” 2025. CIMIC-COE Handbook. https://www.cimic-coe.org/handbook-entries/welcome-to-the-cimic-handbook/vii-resilience/.

- “STEADFAST DART – STDT25 Factsheet.” 2025. Joint-Forces.com, 10 January. https://www.joint-forces.com/exercise-news/78965-steadfast-dart-stdt25-factsheet.

- “Strategic Concept.” 2022. NATO. https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf.

- “The U.S. Army in Multidomain Operations 2028.” 2018. TRADOC Pamphlet 525-3-1. https://adminpubs.tradoc.army.mil/pamphlets/TP525-3-1.pdf.

- “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies.” 1967. United Nations Office for Outer Space Affairs. https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html.

OPEN
PUBLICATIONS

Day Zero Integration and
Multi-Domain Operations
www.openpublications.org