Atlantic Council

SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

THE FUTURE OF NATO C4ISR

Assessment and Recommendations After Madrid

Gordon B. “Skip” Davis Jr.

The Scowcroft Center for Strategy and Security works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The Scowcroft Center's Transatlantic Security Initiative brings together top policymakers, government and military officials, business leaders, and senior experts from Europe and North America to share insights and develop innovative approaches to the key challenges facing NATO and the transatlantic community.

March 2023

Cover photo: NCI Agency.

ISBN-13: 978-1-61977-273-1

 This publication was produced in partnership with Leonardo DRS, Inc. under the auspices of a project focused on modernizing NATO interoperability.

THE FUTURE OF NATO C4ISR

Assessment and Recommendations After Madrid

FOREWORD

Even as Russia's illegal and unprovoked war in Ukraine rages, the transatlantic community is seeking to integrate lessons from the battlefield to adapt its defense planning for a rapidly changing world. Already, one lesson is clear: In a contested Europe, allies need to have better awareness of the operating environment. The speed and quality of decision-making and execution must improve. Effective and ethical NATO decision-making must be translated into operational effects. NATO must prioritize the modernization and integration of its command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architecture to keep pace with the rapidly changing operational environment.

While a complex concept, C4ISR is most easily understood as the "nervous system" of the military. It is essential to everyday operations, automatic responses, and the complicated processes inherent to large enterprises. Rapid and fundamental changes in our security environment—including the return of large-scale war in Europe, China's growing global ambitions, climate change, and the transformative potential of emerging technologies—require an immediate and critical examination of NATO's C4ISR architecture. Modernizing C4ISR is necessary to maintain a competitive advantage against state-based adversaries, other systemic challenges, and threats yet to materialize—all of which could overturn the rules-based international order NATO is dedicated to preserving.

The platform offered by NATO's new Strategic Concept for strengthening defense and deterrence while leveraging emerging and disruptive technologies provides a unique window of opportunity for transatlantic decision-makers. It is NATO's C4ISR capabilities that will enable a relevant and credible NATO "nervous system" equal to the challenges ahead.

To that end, this study by the Atlantic Council—the culmination of a year of research and interviews by NATO's former deputy assistant secretary general for defense investment—offers a detailed roadmap to achieve this goal. This comprehensive report offers an expert treatment on the topic of C4ISR modernization to help transatlantic decision-makers, operational forces, the expert and policy community, and military technology watchers alike better understand the challenges and opportunities inherent to NATO's C4ISR architecture. Importantly, it imagines the possibilities for C4ISR modernization through a series of thoughtfully considered recommendations.

Ultimately, the question is not whether NATO will need to evolve and develop its C4ISR capabilities, but whether it can do so in time to meet the gathering threats to the Alliance. I believe this extensive study skillfully sets forth the path for the necessary modernization of NATO's C4ISR architecture.

—**Gen. James Cartwright**,
Atlantic Council board director and former vice chairman of the Joint Chiefs of Staff

PREMISE

NATO needs to urgently respond to changing requirements, leverage the potential of technology and innovation, and address critical issues to provide the command and control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) architecture that Alliance leaders and forces need to maintain their comparative military advantage over the coming decade.

Current C4ISR capabilities, concepts, policies, and processes do not meet all of the Alliance's needs. While much has been done to improve NATO C4ISR over the past decade, much work remains. Russia's war in Ukraine and other threats and challenges, including from China and climate change, have added a sense of urgency to this task. Russian aggression, in particular, has tested some aspects of NATO C4ISR and provided initial lessons learned in terms of its strengths, vulnerabilities, and shortfalls.

NATO has a unique window of opportunity to leverage the current sense of urgency, newfound cohesion among allies, and an agreed vision to build the C4ISR architecture it needs for the future.

NATO needs to first provide a clarifying definition of C4ISR architecture, which does not currently exist. A defined C4ISR architecture would harmonize defense planning efforts across multiple domains, enable aggregation and assessment of related capability targets, and ensure greater coherence in concept and capability development.

The trajectory of NATO C4ISR is impacted by political ambitions. These include Digital Transformation, increasing resilience, understanding the security implications of climate change, reducing defense impacts on climate change (e.g., reducing the use of fossil fuels, energy consumption, carbon emissions, toxic waste, and contaminants), and raising the level of NATO common funding.

Political decisions and ambitions announced in the June 2022 Madrid Summit Declaration and NATO 2022 Strategic Concept—the most important of which include those related to strengthening deterrence and defense and increasing focus on innovation and emerging and disruptive technologies—will shape the NATO C4ISR architecture of the future.

INTRODUCTION

The context of European security and defense has drastically changed since Russia invaded Ukraine on February 24, 2022. The war has upended conventional wisdom on Russia's willingness to use violence, exposed the destructiveness of modern weapons and barbarity of an undisciplined force, and revealed Russian hubris and the limits of Russian power.

On the flip side, the war has strengthened the bond between NATO and the European Union (EU). NATO and EU leaders have taken an unprecedented level of coordinated decisions and actions to impose costs on Russia, defend Europe from further aggression, and support Ukraine in its battle for survival and independence. Alliance and EU leaders have also begun to seriously address other challenges affecting security, such as energy, climate change, and China.

Russia's war has highlighted the power of united action while exposing the limits of Alliance adaptation to date and identifying vulnerabilities and shortfalls that allies and EU member states must address to ensure their security and defense.

More than ever, the speed of understanding, decision-making, and action are important in modern warfare. Russia has demonstrated on multiple occasions over the past fifteen years that it is capable of rapid decision-making, assembly, and maneuver that has arguably challenged NATO's ability to respond at the speed of relevance. Georgia in 2008, Ukraine in 2014, annual strategic exercises, and frequent combat readiness tests are all examples.

NATO has improved intelligence sharing and its defense posture since 2014, the year Russia annexed the Crimean Peninsula from Ukraine and began its support to separatists in the Donbas. These improvements have enabled a cohesive and coherent NATO response to the Russian military buildup in 2021 and subsequent invasion of Ukraine in 2022. Whether NATO can effectively identify, prepare for, and defend against Russian aggression toward an ally anywhere in Europe without significant additional posture adjustments is in question.[1]

NATO command and control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) structures, capabilities, and processes enable effective political and military awareness, decision-making, and action.[2] These capabilities encompass an array of land, air, maritime, cyber, and space systems, platforms, and applications that can be owned and operated by all thirty allies (which may soon be thirty-two with Finland and Sweden joining the Alliance),[3] by a group of allies (e.g., multinational formations), or by single nations contributing to NATO missions, operations, and activities.

Despite a growth in collective and national capabilities over the past ten years, NATO C4ISR capabilities remain under resourced, vulnerable, and much less effective than required. Supporting concepts, policies, and procedures related to NATO C4ISR need urgent revision. Many are under development. NATO is engaging industry and the broader private sector, but the latter's role is not yet fully leveraged. In its current state, NATO C4ISR will be severely challenged to guarantee the security and defense of the Alliance against the threats and challenges it expects to face over the coming decade.[4]

The time to act is now. NATO allies currently enjoy unprecedented cohesion, share an agreed and clear vision for the future, and are motivated by a common sense of urgency, all imbued by the ongoing Russian war on Ukraine. Defense investment is rising and the foundations of a future C4ISR architecture and its components are in various stages of development or planning.

---

1 Scowcroft Center Task Force for Deterrence and Force Posture, *Defending Every Inch of NATO Territory: Force Posture Options for Strengthening Deterrence in Europe*, *Atlantic Council*, March 9, 2022, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/us-and-nato-force-posture-options/.

2 For this report, information technology (IT), including services, are included in the categories of "communications" and "computers." While some countries include cyber as a related capability category (i.e., C5ISR), NATO treats cyber as an operational domain (cyberspace) and an enabling capability for C4ISR.

3 NATO, "NATO Allies Sign Protocols for Accession of Finland and Sweden," last updated July 5, 2022, https://www.nato.int/cps/en/natohq/news_197763.htm.

4 NATO, NATO 2022 Strategic Concept, June 29, 2022, 3-6, https://www.nato.int/strategic-concept/#StrategicConcept.

NATO Secretary General Jens Stoltenberg displays the Strategic Concept booklet during his news conference at a NATO summit in Madrid, Spain June 29, 2022. Photo by Susana Vera via REUTERS.

NATO and national capabilities must be interoperable and more integrated within and across domains to deliver multidomain effects. The Alliance needs a modern and well-defined C4ISR architecture to achieve its ambition of securing and defending the Alliance and its interests. NATO must improve and further enable its C4ISR with common structure, policies, concepts, frameworks, standards, procedures, and connectivity. NATO must also modernize and integrate current capabilities and acquire new capabilities. Allies need to further increase sharing of data and intelligence, interoperability, and national contributions (forces, platforms, systems, people, and resources) to strengthen NATO C4ISR.

To maintain a comparative advantage against potential adversaries and challengers, NATO allies must

1) share more data and intelligence;
2) transform digitally;
3) implement new concepts, policies, and plans to clarify C4ISR requirements;
4) modernize, augment, and acquire capabilities to meet new C4ISR requirements; and
5) continue to invest in C4ISR interoperability, readiness, resilience, innovation, and adaptation.

THREATS AND CHALLENGES SHAPING NATO C4ISR

Russia's war against Ukraine is a major inflection point for NATO, which is in the midst of a long-term effort to improve its deterrence and defense. NATO's response to Russian aggression has been to assure and defend allies, deter Russia, and support Ukraine. This response has included a surge in the employment of NATO-owned C4ISR forces such as the NATO Alliance Ground Surveillance Force (NAGSF);[5] still at Initial Operational Capability) and the NATO Airborne Early Warning and Control Force (NAEW&CF).[6] National joint intelligence, surveillance, and reconnaissance (JISR) assets have contributed to Alliance shared awareness. NATO cooperation with the EU has led to a united front in communications and complementary actions by EU and non-EU allies on sanctions against Russia, energy security, and support to Ukraine.

Russia "poses the most significant and direct threat" to NATO,[7] **but there are other threats and challenges that the Alliance must also face or prepare for**. Other threats identified by NATO include terrorism in all its forms, missiles from Iran, and cyber and hybrid attacks. All of these threats require constant vigilance, early warning, intelligence, rapid response, and defense and security capabilities enabled by NATO C4ISR.

Among the challenges identified by NATO, China and climate change are the most significant, along with regional instability and strategic shocks. China's policies and its rising economic, financial, diplomatic, informational, and military power pose a multitude of challenges to NATO's security, interests, and values. NATO C4ISR must enable shared awareness of China's policies, actions, and growing military and civilian capabilities. NATO C4ISR must be resilient and respond to Chinese cyber and hybrid activities and favorably compete with Chinese technological advancements and norm-setting efforts.

With respect to climate, NATO C4ISR must contribute to awareness and understanding of the security implications of climate change and contribute to the reduction and mitigation of adverse impacts on climate. Similarly, NATO C4ISR must be able to contribute to anticipation and response related to regional instability and strategic shocks. The addition of crisis prevention to the previous core task of crisis management in the 2022 Strategic Concept highlights a NATO ambition to ensure sufficient awareness (only provided by an effective C4ISR architecture) to understand potential challenges in time to proactively shape, attenuate, or mitigate them.

Preparing for and facing the other threats and challenges listed above implies an ability to cooperate with a broad range of partner organizations and nations, including sharing information and intelligence, and an adequate level of interoperability for coordinated responses. Interaction and combined action with partners will both contribute to and set demands on NATO C4ISR.

---

5 NATO Air Command, "NATO Alliance Ground Surveillance Force takes over critical infrastructure," November 28, 2022, https://ac.nato.int/archive/2022/NAGSF_new_infra.

6 NATO Air Command, "NATO Airborne Early Warning and Control," accessed February 16, 2023, https://ac.nato.int/missions/indications-and-warnings/AWACS.

7 NATO 2022 Strategic, "Strategic Environment," 4.

LESSONS FROM THE RUSSIA-UKRAINE WAR FOR NATO C4ISR AND FUTURE NEEDS

The ongoing Russian war in Ukraine is providing a treasure trove of lessons for NATO. NATO is still gathering, processing, and internalizing these lessons, but many are already evident. Some are already captured in reports and articles from journalists, academia, industry, and civilian and military leaders. After reviewing open sources and interviewing several NATO civilian and military leaders, I have assembled the following lessons as most relevant to the future development of NATO C4ISR.

Muti-domain operations.

NATO C4ISR must be able to support multi-domain operations (MDO) and deliver multi-domain effects. Much work in connectivity, integration, and interoperability is needed.

The Russian war on Ukraine is the first of its scale in Europe in the twenty-first century. No other recent conflict in Europe—Russia's war on Georgia in 2008 or Ukraine from 2014 to February 24, 2022—has involved a similar number of military forces or employed such destructive power. Russia and Ukraine have employed or leveraged capabilities in all five domains—air, land, maritime, cyberspace, and space. Russia has struggled with coordinating joint action, let alone achieving multi-domain effects. "Russia has definitely showed us how not to fight," said Rear Adm. Nicholas Wheeler, director of NATO Headquarters C3 Staff (NHQC3S).[8] Ukraine appears to have had more success leveraging multi-domain capabilities. Ukrainian forces have effectively targeted and engaged Russian land and maritime forces using limited multi-source intelligence, aerial drones, maneuver and fires units, and commercial space-based open-source intelligence (OSINT) services from a variety of private companies.

Figure 1. The Five NATO Operational Domains

Iconography credit: fahmionline, Muhammad Shayan, GreenHill, Creative Mania, Edi Prastyo.

The Russian war in Ukraine is a likely catalyst for NATO leaders to hasten the development of an Alliance MDO Concept. Additionally, NATO's 2022 Strategic Concept highlights the importance of multi-domain forces and warfighting.[9] NATO has added cyber and space as operational domains over the past decade and has been working on an MDO concept for some time.[10] Allied Command Transformation (ACT) and Allied Command Operations (ACO) delivered an Initial Alliance Concept for MDO in July 2022.[11] NATO's "working definition" of MDO is "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."[12]

8 Rear Adm. Nicholas Wheeler, interview by author, August 16, 2022.

9 NATO 2022 Strategic, 6.

10 Allied Command Transformation (ACT) began talks in June 2021. See Lieutenant Colonel Jose Diaz de Leon, "Understanding Multi-Domain Operations in NATO," *Three Swords Magazine* 37 (2021), 92, https://www.jwc.nato.int/application/files/1516/3281/0425/issue37_21.pdf. During the author's assignment to Allied Command Operations (ACO), from 2013 to 2015, staff officers in the Supreme Headquarters Allied Powers Europe (SHAPE) Plans Directorate developed a draft definition and concept for MDO that was shared with senior SHAPE staff.

11 Allied Command Transformation (ACT), "Multi-Domain Operations: Enabling NATO to Out-Pace and Out-Think Its Adversaries," July 29, 2022, https://www.act.nato.int/articles/multi-domain-operations-out-pacing-and-out-thinking-nato-adversaries.

12 Ibid.

According to Headquarters (HQ) Supreme Allied Commander Transformation (SACT) Deputy Chief of Staff (DCOS) for Capability Development Lt. Gen. David Julazadeh, NATO leaders have directed the Strategic Commands to accelerate delivery and implementation of an Alliance MDO Concept.[13]

Day zero readiness.

The scale of Russia's military buildup and geographically broad and rapid employment of force against Ukraine have caused NATO civilian and military leaders to question whether the Alliance's current plans and defense posture would have deterred or rapidly repelled a similar Russian assault against an ally, particularly a small nation.[14] Could NATO respond with the speed, scale, and coherence needed to prevent initial success?

Two ongoing efforts will help. First, a new Supreme Allied Commander Europe's (SACEUR's) Area of Responsibility (AOR)-Wide Strategic Plan (SASP) was approved earlier in 2022, but the underlying regional and subordinate strategic plans have yet to be completed and stitched together. Second, a new NATO Force Model approved at the Madrid Summit in June 2022 will address much of the speed, scale, and coherence lacking in current policies and posture by assigning a much larger number of forces (up to four hundred thousand) to regional plans.

Day zero readiness. An informal NATO term referring to being mission-ready on the first day of a NATO mission (e.g. a network, a force, a headquarters).

Other efforts are in the works. The adapted command and control (C2) structure is not yet fit for purpose and ACO has been directed to conduct a comprehensive C2 assessment. NATO's Air Command and Control System (ACCS) is woefully behind the times, and a transition plan to a future Air C2 system is in development. According to NATO Assistant Secretary General (ASG) for Operations Tom Goffus: "The NATO Crisis Response System [NCRS] was designed for out of area operations where NATO drives the timeline and has the luxury of time. Now we don't have that time advantage."[15] The NCRS needs significant revision to enable day zero readiness for collective defense. Goffus is determined to drive such a revision.

The family of plans under development, the new NATO Force Model, and revised C2 structure and NCRS will influence future requirements for NATO C4ISR. NATO must review and update C4ISR requirements for standing defense and baseline activities, as well as exercise and enable rapid activation and deployment related to a short to no-notice collective defense scenario.

NATO Intelligence Enterprise (NIE).

The NATO Intelligence Enterprise (NIE) surged, adapted, and delivered the intelligence political and senior military leaders needed to respond to the Russian war in Ukraine.[16] This is good news. The decisions post-2014 to establish the NATO HQ Joint Intelligence and Security Division (JISD), increase JISR capabilities, and improve NATO's indicators and warnings (I&W) system have all been validated. The capabilities and processes were not always ideal, but holistically the NIE enabled cohesion, collective decision-making, an effective military response, and effective communications for aggression against a partner nation. The bad news is these outcomes are related to, but not sufficient for, defense against a peer adversary.

NIE's ability to function and deliver in a collective defense, multi-domain, and high-intensity combat situation requires further improvements in the C4ISR architecture.

NATO-owned C4ISR capabilities like the Alliance Ground Surveillance[17] (AGS) and Airborne Early Warning and Control System[18] (AWACS) have proven their value in the current conflict in Ukraine, yet operations have exposed limitations in readiness, types of sensors, quantity of platforms, and

13 Lt. Gen. David Julazadeh, interview by author, August 2, 2022.

14 The author defines defense posture as the whole of command and control (C2) structures, baseline activities for deterrence and defense, force readiness, responsiveness, reinforcement plans, and capabilities.

15 Tom Goffus, interview by author, July 15, 2022.

16 David Cattler, interview by author, July 13, 2022, and Maj. Gen. Philip Stewart, interview by author, July 11, 2022.

17 NATO, "Alliance Ground Surveillance (AGS)," last updated July 20, 2022, https://www.nato.int/cps/en/natohq/topics_48892.htm.

18 Airforce Technology, "E-3 AWACS (Sentry) Airborne Early Warning and Control System," June 25, 2020, https://www.airforce-technology.com/projects/e3awacs/.

NATO's Alliance Ground Surveillance (AGS) RQ-4D ''Phoenix'' remotely piloted aircraft. Photo by NATO.

connectivity.[19] NATO ASG for Intelligence and Security David Cattler highlighted the positive: "NATO and nations contributed with data, platforms, and intelligence. The US shared and declassified intelligence in an unprecedented way and even small nations responded and contributed to specific requirements. Strategic and operational intelligence provided to allies was well coordinated between JISD and ACO."[20] That said, personalities drove much of the success in overcoming standing C4ISR issues in terms of sharing, declassification, coordination procedures between NATO HQ and ACO, and related budgetary issues.[21]

Persistence and survivability.

One clear lesson from the Russian invasion of Ukraine, said former ACO DCOS Strategic Employment Maj. Gen. Philip Stewart, "is the need for persistent surveillance."[22] Persistent surveillance is fundamental for effective NATO deterrence and defense and crisis prevention and management because it provides military and political leaders the near-real-time awareness of threat I&W that enable timely decision-making and action. The ability to see and communicate the Russian buildup, invasion, and military action at the operational and tactical levels enabled shared awareness, decision-making, and response. The allies had the luxury of time in the case of Ukraine.

To ensure an effective response against a highly capable peer adversary, NATO needs persistent surveillance, which requires new structures, policies, processes, and capabilities. Persistent surveillance will likely demand a combination of assets from multiple domains. According to NATO ASG for Defense Investment (DI) Camille Grand, "The ability to use and fuse different tools will be critical to achieve

19 Stewart, interview and Brig. Gen. Houston Cantwell, interview by author, July 8, 2022.

20 Cattler, interview.

21 Ibid. and Stewart, interview.

22 Stewart, interview.

persistent surveillance."[23] Both Russian and Ukrainian combatants have employed a vast array of drones, from high and medium-altitude long-endurance platforms to small and very small systems, with an array of capabilities for a variety of missions (including intelligence, surveillance, and reconnaissance, or ISR, and target acquisition). Increases in dedicated NATO and national capabilities from space, high, medium, and low altitude are needed to respond to strategic and operational intelligence requirements in a collective defense scenario.

"The Alliance needs robust, in-depth, and survivable JISR platforms in the future," Cattler said.[24] Survivability of NATO C4ISR in modern warfare against a peer adversary is a critical requirement. NATO-owned AGS RQ-4s and AWACS E3As have limited survivability in a contested environment. NATO and national tactical communications are vulnerable to adversary electronic warfare (EW) capabilities. Future solutions may come from a combination of greater sensor range, stealth characteristics, electronic countermeasures, other performance characteristics, or next generation communications systems. Survivability of non-deployable and deployable NATO C2 is another aspect highlighted by the destructive effect of missiles employed in the Russia-Ukraine war. Passive measures like dispersion, displacement, alternate locations, concealment, and degraded operational procedures are all being reviewed or planned. Active measures like air and missile defense planning and deployment to protect NATO C2, not so much. That said, NATO has increased its air and missile defense posture along its eastern flank in the form of short deployments of air and land assets under NATO's Air Shielding mission.[25]

Space-based intelligence (as well as other space-based services like communications, early warning, tracking, and guidance) offers a partial answer to the need for both persistent surveillance and survivability, as space-based capabilities are expected to expand rapidly in the coming years.[26] National, military, and commercial space-based intelligence (imagery, communications, and electronic signatures) has the potential to contribute greatly to persistent surveillance. NATO will be more and more interested in protection, durability, and survivability of space-based assets, which must be addressed by nations and industry. Redundancy in space-based sensors and assets and the decreasing cost of replacement and remote maintenance may offset some of the need for survivability.

Multidisciplinary intelligence and fusion.

Imagery intelligence (IMINT), signals intelligence (SIGINT),[27] and OSINT played a key role in unmasking Russian intent and disinformation from the national to tactical level, as well as in targeting. Allies, NATO, Ukraine, and Russia have all exploited space-based data and information (imagery, signals, signatures) for intelligence analysis and production. Ukraine has combined commercially available space-based data and crowdsourced information (technically both part of OSINT) to effectively identify and engage key Russian targets (e.g., leadership, C2 and logistic nodes, and major platforms), refute Russian official narratives, and identify war crimes and war criminals.

There is a need for improvements in NATO's multidisciplinary intelligence capabilities and ability to collect, fuse, and process such intelligence. The Alliance has powerful all-weather sensors in its NATO-owned AGS (Synthetic Aperture Radar, Ground Movement Target Indicator), but no electrical-optical (EO), infrared (IR), full-motion video (FMV), or SIGINT capabilities.[28] The latter capabilities are key for collective defense and a broad range of other crisis and security operations. NATO SIGINT (provided through national contributions) has contributed to strategic shared awareness and decision-making but is still too compartmentalized and often overclassified to be fused and used meaningfully at the operational and tactical levels. NATO has no NATO-owned

23 Camille Grand, interview by author, August 1, 2022.

24 Cattler, interview.

25 "Video: 5 Things You Should Know about NATO's Air Shielding Mission," SHAPE, August 19, 2022, https://shape.nato.int/news-archive/2022/video-5-things-you-should-know-about-natos-air-shielding-mission.

26 Mattia Olivari, "The Space Sector: Current Trends and Future Evolutions," ISPI, December 11, 2021, https://www.ispionline.it/en/publication/space-sector-current-trends-and-future-evolutions-28602.

27 Signals intelligence (SIGINT) is composed of communications intelligence (COMINT) and electronic intelligence (ELINT).

28 NATO's E-3A AWACS has a look down surveillance radar that collects measurement and signature intelligence (MASINT), but not COMINT. See Airforce Technology, "E-3 AWACS (Sentry) Airborne Warning and Control System," June 25, 2020, https://www.airforce-technology.com/projects/e3awacs/.

SIGINT sensors or platforms, and its EW capabilities are a long-standing shortfall at the tactical level.

Two initiatives underway can partially address NATO's need for SIGINT and OSINT. First, the Alliance Persistent Space Surveillance[29] (APSS) initiative set up in April 2022 and formally launched in February 2023 is a key step toward enabling NATO's collection of national contributions and commercial contracting of space-based data, products, and services.[30] Second, the NATO Public Diplomacy Division's (PDD) Information Environment Assessment (IEA) project (supported by JISD and ACT) is prototyping an artificial intelligence (AI) tool to help NATO professionals sort and analyze vast amounts of print, media, and online information.[31] The APSS and IEA initiatives deserve expansion and acceleration in delivery to meet NATO's current and future C4ISR needs.

Tasking, Collection, Processing, Exploitation, and Dissemination (TCPED).

TCPED is the information management process that NATO and other military or government organizations use to synchronize intelligence and operational efforts to acquire and deliver intelligence in response to specific requirements.[32] An effective and responsive TCPED process is fundamental to NATO's ability to deliver timely and relevant intelligence in response to strategic political and operational military demands. The NIE's response to the Russia-Ukraine crisis as well as observations of the combatants in the war have highlighted the need for vastly improved capacity for TCPED.

NATO's TCPED process is operating at a level below its potential and short of strategic and operational need. Speed and efficiency of the TCPED process are already challenged by current levels of structure, data, assets, and analysts. According to NAEW&C Force Commander Maj. Gen. Tom Kunkel, "NATO leaves so much data on the cutting floor."[33] Matters would only be worse if NATO were fully engaged in a modern conflict attempting to execute MDO.

AI and machine learning (ML) tools, along with improved data management and connectivity, could offer relatively cheap solutions (as opposed to major equipment programs) to vastly improve the speed, efficiency, and effectiveness of the NATO TCPED process (from the strategic to tactical levels).

Cyber.

The role of cyber in the Russia-Ukraine war has been surprising. Pre-invasion, leaders and analysts generally expected the Ukrainian government and military to succumb to the crippling effects of Russia's "overwhelming" cyber capabilities. That has not happened.

According to Cattler, open sources reveal that Russia deployed destructive cyber malware against Ukrainian government and military C2, rendered systems inoperable, and sabotaged an Internet provider that both Ukrainian police and military depend on. All of this was evidence of "good cyber reconnaissance ahead of time by Russia," he said.[34] However, he added, Russian cyber operations were "not coordinated with conventional ops" nor exploited.[35] The reasons are likely a mix of restraint on the part of Russia; a limited ability of Russia to coordinate cyber and other domain effects; the competence of Ukrainian military, government, and private citizens in restoring and protecting systems and services; and significant assistance to Ukraine from powerful private companies like SpaceX and Microsoft (see more on this later).

---

29 NATO, "Alliance Persistent Surveillance from Space (APSS)," updated February 2023, https://www.nato.int/nato_static_fl2014/assets/pdf/2023/2/pdf/230215-factsheet-apss.pdf.

30 NATO Communications and Information Agency (NCIA) General Manager Ludwig Decamps, interview by author, July 21, 2022, and Director of Armament and Aerospace Capabilities in NATO's Defense Investment Division Giorgio Cioni, interview by author, August 2, 2022.

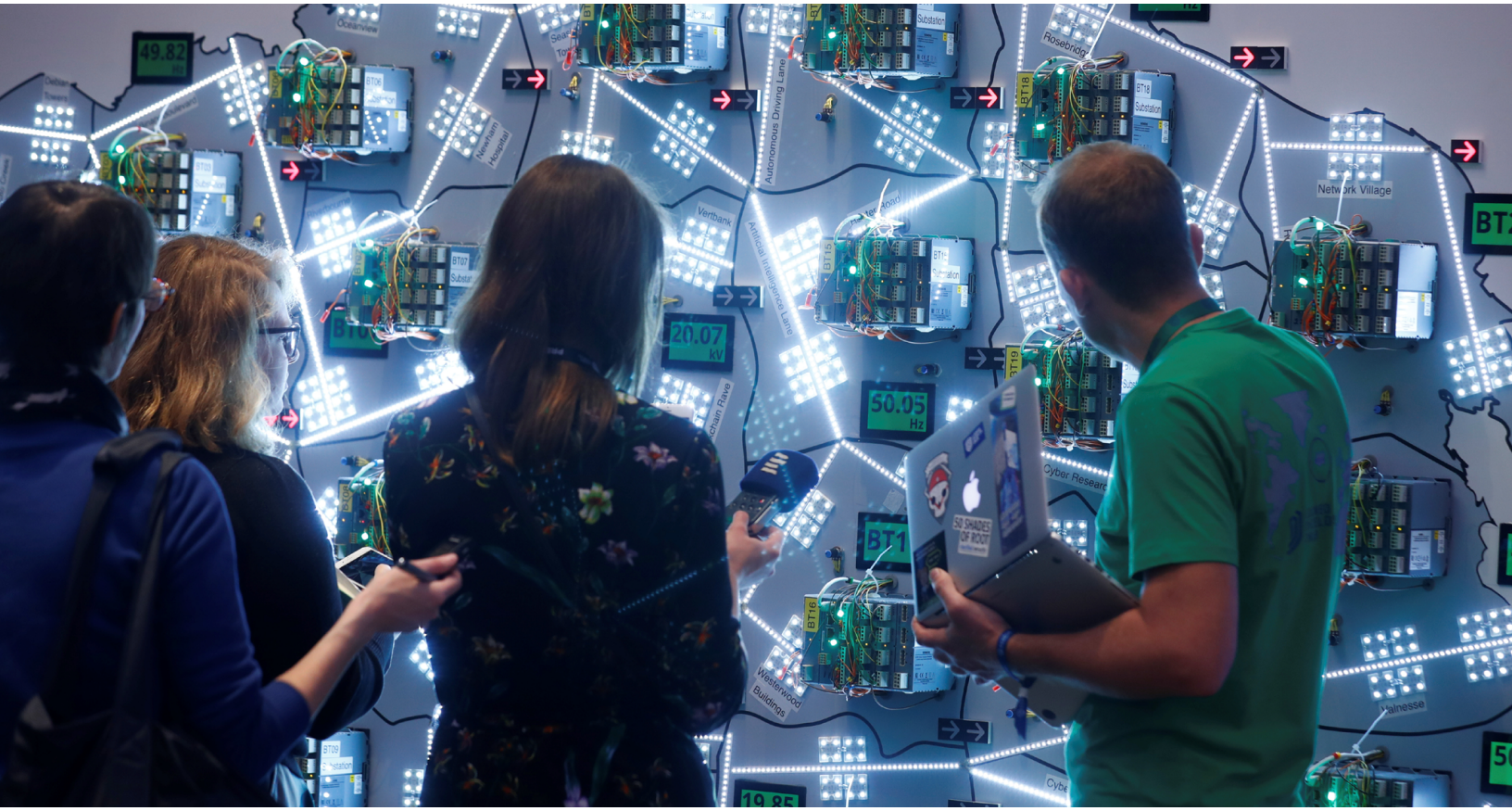
31 Author's personal knowledge from assignment at NATO Headquarters as deputy assistant secretary general (ASG) Defense Investment (DI).

32 NATO uses TCPED in internal documents and communications to refer to the key steps of its intelligence process. The five steps of NATO TCPED are equivalent to what the US Department of Defense describes as the six steps of the "intelligence process": "planning and direction, collection, processing and exploitation, analysis and production, dissemination and integration, and evaluation and feedback." See Department of the Army et al., *Joint Publication 2-01. Joint and National Intelligence Support to Military Operations*, January 5, 2012, GL-10, https://irp.fas.org/doddir/dod/jp2_01.pdf.

33 Maj. Gen. Tom Kunkel, interview by author, August 4, 2022.

34 INSA (Intelligence & National Security Alliance), "Coffee and Conversation with David Cattler," July 25, 2022, YouTube video, https://www.youtube.com/watch?v=b5mJUtnNI88.

35 Ibid.



Locked Shields, cyber defence exercise organized by NATO Cooperative Cyber Defence Centre of Exellence (CCDCOE) in Tallinn, Estonia April 10, 2019. Photo by Ints Kalnins via REUTERS.

There are also limits to cyber effects. Chief of Britain's General Staff, Gen. Patrick Sanders, said: "You can't cyber your way across a river."[36] But you might be able to stop a river crossing (see more on this later). While cyber-related lessons from Russia's war on Ukraine have yet to be comprehensively gathered, Cattler said: "Allies have recognized that cyberspace is contested at all times and cyber defense underpins the broader deterrence and defense posture."[37] Cyberspace is an enabler of C4ISR and an operational domain for cyber operations, activities, and effects related to C4ISR. Cyber represents great potential and opportunities as well as risk and vulnerabilities. NATO must build cyber resilience in its C4ISR architecture and capabilities, leverage private sector expertise and services, and incorporate voluntary national contributions of cyber ISR.

The role of private industry.

Private industry has played an outsized role in enabling the Ukrainian response to the Russian aggression, and providing security, resilience, communications, and intelligence to Ukraine and allies alike—all key elements and enablers of C4ISR. SpaceX's decision to provide thousands of Starlink terminals to enable satellite communications and Internet services for Ukrainian private and public users has been a game changer.[38] Microsoft's support to Ukraine and other countries under Russian cyberattack has enabled understanding of the threat, capabilities to secure data and networks and enable resilience, and provided a comprehensive strategy for response.[39] According to NATO ASG for Emerging Security Challenges David van Weel,

36 Daniel Michaels, "Lessons of Russia's War in Ukraine: You Can't Hide and Weapons Stockpiles Are Essential," *Wall Street Journal*, July 4, 2022, https://www.wsj.com/articles/lessons-of-russias-war-in-ukraine-you-cant-hide-and-weapons-stockpiles-are-essential-11656927182.

37 INSA, "Coffee and Conversation."

38 Michael Sheetz, "Elon Musk's SpaceX Sent Thousands of Starlink Satellite Internet Dishes to Ukraine, Company's President Says," CNBC, March 22, 2022, https://www.cnbc.com/2022/03/22/elon-musk-spacex-thousands-of-starlink-satellite-dishes-sent-to-ukraine.html.

39 Microsoft, *Defending Ukraine: Early Lessons from the Cyber War*, June 22, 2022, 4, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE50KOK.

Microsoft's talent, expertise, and tools are critical for NATO cyber defense and data management.[40]

Private companies like Maxar, BlackSky, and Planet (imagery) and HawkEye 360 (signals) are providing AI-enabled space-based services to Ukraine and NATO allies.[41] Commercial data, information, and services provided to Ukraine and the allies have been used to confirm Russian military locations and actions (including atrocities and war crimes) and refute disinformation. According to Van Weel, one commercial AI tool is being prototyped by the NATO Intelligence Fusion Center[42] (NIFC) to save hours of costly analyst time spent counting aircraft from massive amounts of collected imagery. This tool has enabled near-real-time analysis of Russian air assets and battle damage as well as cueing of changes to existing status.[43]

NATO Communications and Information Agency (NCIA) General Manager Ludwig Decamps offered that "perhaps we need to add industry as another domain of operations."[44] Noting that NATO already depends on industry for critical services and innovative responses to military need, Decamps added: "How do we include in our planning to account for industry's expertise, inherent responsibilities, and potential contributions?"[45] NATO engagement with industry includes a robust relationship through the NATO Industrial Advisory Group (NIAG),[46] which includes national industry delegations from all allies, and recently launched NATO initiatives like Defense Innovation Accelerator for the North Atlantic (DIANA)[47] and the NATO Innovation Fund.[48]

There have been several NATO initiatives and policy efforts over the past five years to increase engagement with parts of the private sector that produce some of the most advanced and innovative technologies. Developed for commercial use, these technologies could also respond to defense requirements.

Until recently, many start-ups and small and medium-sized enterprises (SMEs) rarely engaged with NATO for a variety of reasons, including lack of visibility of NATO needs, lack of experience in NATO procurement processes, concerns over the capital investment needed to compete, and a general view that NATO focused on large, complex systems that were the bailiwick of major primes or consortiums of traditional defense industry.[49]

NATO-Industry Forums (NIFs),[50] multinational cooperation in capability development,[51] internal NATO HQ trials,[52] ACT innovation initiatives,[53] NCIA industry key events,[54] and NATO policy efforts to address emerging and disruptive technologies (EDTs)[55] are all examples of NATO engaging nontraditional industry partners to leverage their creative and innovation potential. Among this broad list of efforts, multinational cooperation in capability

40 David van Weel, interview by author, August 18, 2022.

41 Tara Copp, "Satellite Firms Are Helping Debunk Russian Claims, Intel Chief Says," *Defense One*, April 5, 2022, https://www.defenseone.com/business/2022/04/satellite-firms-helped-debunk-russian-claims-intel-chief-says/364060/.

42 NATO Intelligence Fusion Centre, "NATO Intelligence Fusion Centre," accessed February 16, 2023, https://web.ifc.bices.org/.

43 Van Weel, interview.

44 Decamps, interview.

45 Ibid.

46 NATO, "NATO Communications and Information Agency," https://www.ncia.nato.int/.

47 NATO, "NATO approves 2023 strategic direction for new innovation accelerator," last updated December 21, 2022, https://www.nato.int/cps/en/natohq/news_210393.htm.

48 NATO, Brussels Summit Communiqué, press release, last updated July 1, 2022, https://www.nato.int/cps/en/natohq/news_185000.htm; NATO, "NATO Launches Innovation Fund," last updated June 30, 2022, https://www.nato.int/cps/en/natohq/news_197494.htm.

49 Author's notes from NATO-Industry Forums (NIFs) 2018 and 2019 and post-NIF reports co-published by SACT and ASG DI internally after the event and edited by the author.

50 NIFs 2018, 2019, and 2021 specifically focused on innovation, emerging technologies, and inviting start-ups and SMEs. See references to NIFs 2019 and 2021 in NATO, "NATO-Industry Forum," accessed October 3, 2022, https://www.act.nato.int/industryforum.

51 NATO, "Multinational Capability Cooperation," last updated November 18, 2022, https://www.nato.int/cps/en/natohq/topics_163289.htm.

52 While assigned to NATO HQ, the author sponsored, enabled, or was aware of several trials leveraging advanced technology in AI and data services to demonstrate private sector capabilities to assist in security or defense-related requirements such as: tracking COVID-19-related factors impacting allies, foreign investment in allied defense industry and critical infrastructure, and tracking and analyzing open-source information related to threats.

53 ACT, "Innovation Hub," accessed October 2, 2022, https://www.innovationhub-act.org.

54 NATO Communications and Information Agency, "Our Key Events," accessed October 2, 2002, https://www.ncia.nato.int/business/partnerships/key-events.html.

55 NATO, "NATO Sharpens Technological Edge with Innovation Initiatives," last updated April 7, 2022, https://www.nato.int/cps/en/natohq/news_194587.htm.

Local residents use a Starlink terminal, amid Russia's attack on Ukraine, in Chasiv Yar, Donetsk region, Ukraine January 31, 2023. Photo by Oleksandr Ratushniak via REUTERS.

development has provided the most concrete, albeit still limited, results. DIANA, specifically, will focus on engaging and leveraging start-ups and SMEs, which until recently (prior to 2019) had been under-represented or less represented in NATO engagements with industry.[56]

The importance of these initiatives in engaging the private sector and leveraging its technology, innovation, and expertise, including that of promising start-ups and SMEs, to develop creative solutions to NATO military problems at pace has only grown due to the ongoing war in Ukraine.

Digitalization, connectivity, and Big Data.

Interrelated to many of the previous lessons identified are the importance of digitalization of information (including signals, print, and electronic media), connectivity (efficient, secure, robust, and resilient networks), common data frameworks (standard protocols and interfaces), and data management tools to enable data sharing and Big Data exploitation. More comprehensive intelligence analysis (as well as research in general) has long been hampered by several limitations: the number of documents or signals available in digital form, disconnected private and public data silos containing exploitable information, the lack of common protocols and interfaces to access and share data, and the lack of data management tools in general. While data management and cloud services have become the norm in the private sector, the public defense sector has been wary and slow to adopt. But necessity is the mother of invention and Ukraine is a particularly relevant proving ground.

A prominent example of digitally enabled C4ISR that has been used to rapidly target and destroy Russian forces is the Ukrainian-developed and British-

56 Ibid.

enabled GIS Arta application.[57] Described as "Uber-style technology" providing situational awareness and rapid targeting, the system is fed by "real-time battlefield data from reconnaissance drones, rangefinders, smartphones, GPS [global positioning system] and NATO-donated radars."[58] The system then identifies targets and "rapidly selects artillery, mortar, missile or combat drone units that are within range."[59] Rapid calculation of firing options and alerting of firing units has cut the (Ukrainian) military's targeting time from twenty minutes to one.[60]

Microsoft's ability to connect, secure, and exploit data globally is another example of effective Big Data management and exploitation. While digitalization is proceeding, NATO connectivity currently falls short of requirements to effectively link NATO HQ, commands, forces, other bodies, and nations in peacetime, let alone crisis or conflict. A common data framework is not yet operational, data management tools are rudimentary, and data sharing is far below potential. Former NATO Director General of the International Military Staff (DGIMS) Lt. Gen. Hans-Werner Wiermann advocated for a NATO digital backbone to enable connectivity and a military Internet of Things (IoT) to connect C2, systems, sensors, and shooters. The envisioned military IoT would support applications for all manner of military assessment, planning, coordination, and execution functions.[61]

As a result of impetus from the Russia-Ukraine war, other NATO efforts, and productive collaboration across NATO HQ and Strategic Commands, Wiermann's ambition expanded to a more comprehensive Digital Transformation (DT) concept.[62] This DT concept would address digitalization, connectivity, data frameworks, and management tools across the NATO Enterprise. According to Julazadeh, "The nascent NATO DT effort is similar to the US Joint All Domain Command and Control (JADC2) effort, but a bit broader as it encompasses transforming people, processes, and technology. DT is recognized as a sine qua non component of NATO MDO."[63] NATO DT will also enable the design of a future NATO C4ISR architecture.

RUSSIA-UKRAINE WAR LESSONS FOR NATO C4ISR

- Multi-domain operations
- Day zero readiness
- NIE surged, adapted, and delivered
- Persistence and survivability
- Multidisciplinary intelligence and fusion
- Tasking, Collection, Processing, Exploitation, and Dissemination
- Cyber
- Role of private industry
- Digitalization, connectivity, and Big Data

This is not a complete list of lessons relating to C4ISR to be gained from the Russia-Ukraine war, but it provides a good starting point for identifying recommendations for the improvement and further development of NATO C4ISR. Other lessons related to NATO C4ISR, such as the variety of missions autonomous systems can perform, the importance of counter-unmanned aircraft system (C-UAS) capabilities in protecting C4ISR, the importance of EW capabilities, and how to replicate aspects of Ukraine's whole-of-society response to Russian aggression in a whole-of-enterprise NATO effort to adapt, modernize, and transform, will be included in this report's final set of recommendations.

In summary, NATO and the allies have gained valuable lessons related to C4ISR from the Alliance's response to Russian aggression and from the employment of C4ISR capabilities by both Russia and Ukraine.

---

57 Charlie Parker, "Uber-Style Technology Helped Ukraine to Destroy Russian Battalion," *Times*, May 14, 2022, https://www.thetimes.co.uk/article/uk-assisted-uber-style-technology-helped-ukraine-to-destroy-russian-battalion-5pxnh6m9p.

58 Ibid.

59 Ibid.

60 Ibid.

61 Lt. Gen. Hans-Werner Wiermann, interview by author, July 21, 2022.

62 Grand, interview.

63 John R. Hoehn, "Joint All-Domain Command and Control (JADC2)," Congressional Research Service, updated January 21, 2022, https://sgp.fas.org/crs/natsec/IF11493.pdf; Julazadeh, interview.

DECISIONS TAKEN AT THE MADRID SUMMIT AND WORK UNDERWAY AFFECTING NATO C4ISR

Russian aggression and other threats and challenges, including from China and climate change, resulted in a historic NATO summit in Madrid in June 2022. A new NATO 2022 Strategic Concept was approved clearly delineating the threats and challenges facing the Alliance, revising NATO's three core tasks (deterrence and defense, crisis prevention and management, and cooperative security), and laying out key lines of effort for adapting the Alliance politically and militarily for 2030 and beyond.[64] **Political decisions and ambitions announced in the Summit Declaration and in the Strategic Concept, the most important of which include those related to achieving a strengthened deterrence and defense and an increased focus on innovation and EDTs, will shape the requirements and development of NATO's C4ISR architecture**.

Other political ambitions impacting the trajectory of NATO C4ISR include DT, increased resilience, understanding the security implications of climate change, reducing defense impacts on climate change (e.g., reducing the use of fossil fuels, energy consumption, carbon emissions, toxic waste and contaminants), and increasing the level of NATO common funding.

The following analysis summarizes decisions taken at the Madrid Summit, the expected follow-through on these decisions, and other ongoing adaptation efforts previously decided and impacting NATO C4ISR.

NATO's 2022 Strategic Concept broadly sets the context for C4ISR architecture and requirements in its description of threats and challenges expected over the coming decade, and the political guidance under NATO's three revised core tasks.[65] The concept refers to decisions taken at and prior to the Madrid Summit and has critical implications for the enablement, development, and employment of NATO C4ISR.

Multi-domain warfighting.

NATO's 2022 Strategic Concept sets an ambition for multi-domain warfighting and multi-domain forces.[66] NATO has taken an initial step toward this end by adopting a working definition for MDO (as previously noted).[67] To achieve NATO's level of ambition with respect to multi-domain warfighting several more steps are required, such as an approved Alliance MDO Concept, revised Allied Joint Doctrine, improved awareness of threats and opportunities in all domains, upgrades and improvements in capabilities, and secure use of and access to cyberspace and space capabilities. Multi-domain warfighting also requires trained and educated leaders and professionals, trained and exercised forces in MDO, a data-centric approach, and, above all, a cultural shift and new mindset.[68]

The level of effort will be demanding, but the expected outcome is worth the effort: greater shared understanding, collaboration, and synchronization of capabilities and activities across domains to achieve multi-domain effects. MDO concept development and implementation will be enabled by ACT's Warfare Development Agenda, DT, and NATO initiatives related to innovation and EDTs. According to Julazadeh, HQ SACT DCOS for Capability Development, NATO leaders are pressing for accelerated delivery of an Alliance MDO Concept by 2023.[69] Given the breadth and complexity of MDO and the need for supporting studies this is a stretch goal for NATO's Strategic Commands, but its approval and implementation will be revolutionary for the Alliance. Future C4ISR architecture and capabilities will have to be designed, optimized, integrated, and interoperable to support multi-domain warfighting

64 Atlantic Council Experts, "Our Experts Decipher NATO's New Strategic Concept," *New Atlanticist*, Atlantic Council, June 30, 2022, https://www.atlanticcouncil.org/blogs/new-atlanticist/our-experts-decipher-natos-new-strategic-concept/.

65 NATO 2022 Strategic, 1.

66 NATO 2022 Strategic, 6.

67 "Multi-Domain Operations: Enabling NATO."

68 Based on the author's analysis of an unclassified document, not publicly released. Supreme Headquarters Allied Powers Europe (SHAPE) – HQ SACT, "Bi-Strategic Command, Initial Alliance Concept for Multi-Domain Operations," July 5, 2022.

69 Julazadeh, interview.

and full-spectrum operations at the speed of relevance.

Digital Transformation.

As mentioned earlier, DT is intended to address digitalization, connectivity, data frameworks, and data management tools across the NATO Enterprise. DT is intended to enable significant increases in speed, security, and effectiveness in C2, communications, data analysis, intelligence analysis and dissemination, decision-making, operations, and interoperability. Proceeding along this journey will make NATO more agile, resilient, and capable of seizing and maintaining the initiative in peacetime and conflict.

Much of the vision under development is not new and many strands have been under development for some time. Former NCIA General Manager Kevin Scheid was a strong advocate of digitally transforming NATO and had initiated an effort known as "NCIA's digital endeavor" to modernize and improve the security of NATO's communications and information infrastructure and services.[70] Wiermann, the former NATO DGIMS, advocated for development of a NATO digital backbone, which in his view would constitute the new NATO added value to nations in the information age.[71]

The current effort includes both initiatives and is broader and more ambitious. The effort will address the entire NATO Enterprise and include political approval by nations of a vision in fall 2022 and an implementation plan (ideally with resource assessment) by 2023.[72] According to NHQC3S Deputy Director Marco Criscuolo, a three-step concurrent process (modernization, optimization, and transformation) is necessary to address the complexity and uncertainty of a DT journey.[73]

In brief, in step one—modernization—the current main effort includes continuing modernizing existing capabilities and resourcing ongoing programs and projects such as Information Technology Modernization and related network, data, and cybersecurity initiatives. Step two—optimization—includes reviewing and cohering the numerous and currently disconnected capability programs to build synergies, gain efficiencies, and develop better processes, including adopting current off-the-shelf capabilities. Step three—transformation—begins as NATO gains an understanding of the potential of related technologies and tools, starts to adopt them, then revises structures, processes, and capabilities, and builds in resilience (in cyber, space, and physical infrastructure).[74]

DT will enable connectivity between data pools and access to and exploitation of data across the NATO Enterprise. NATO Enterprise coherence will be driven by top-down guidance and internalized principles (a whole-of-enterprise approach). DT will rely on a new organizational culture and mindset that is digitally savvy and data centric. It will also rely on greater engagement with industry to leverage its expertise and services, and greater integration and interoperability, the latter supported by the active setting and shaping of standards. DT will also rely on an agility in capability development and resource management (budgetary and human capital) and a modern approach to obsolescence management that do not currently exist.

DT will influence and enable the design of future C4ISR architecture and capabilities and improve the integration, connectivity, ability to manage and exploit Big Data, and the quality and speed of C4ISR processes.

Strengthened deterrence and defense posture.

The Alliance's decision to "strengthen our deterrence and defense posture to deny any potential adversary any possible opportunities for aggression"[75] is a major change in strategy and has multiple implications for future NATO C4ISR. In particular, the enhanced NATO posture will increase requirements for persistent surveillance and improved awareness of potential threats, a rapid and more effective intelligence

70 NATO Communications and Information Agency (NCIA), "Digitally Transforming NATO: Our Work Explained," March 19, 2019, https://www.ncia.nato.int/about-us/newsroom/digitally-transforming-nato-our-work-explained-.html.

71 Wiermann, interview.

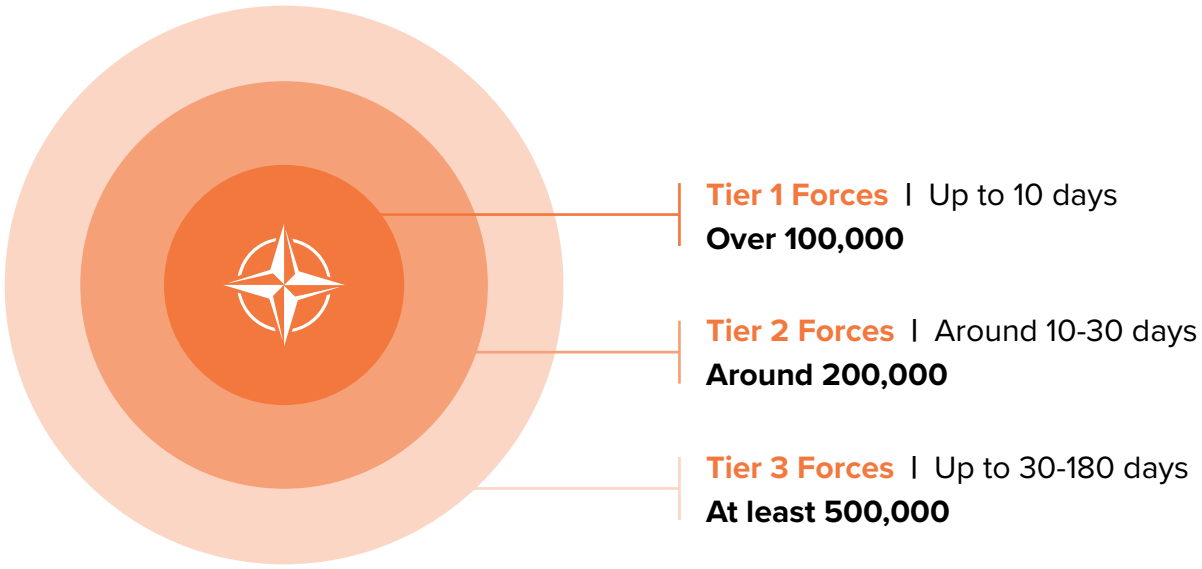
72 Wheeler, interview.

73 Marco Criscuolo, interview by author, August 18, 2022.

74 Wiermann, interview; Criscuolo interview; and Grand, interview.

75 NATO 2022 Strategic, 6.

Figure 2. New NATO Force Model



Credit: NATO.

process, a revised and robust C2 structure, and resilient and secure networks.

A strengthened posture will be enabled by a new NATO Force Model,[76] which will identify and assign around three hundred thousand allied forces at high readiness (ready to move in less than thirty days) to a family of NATO strategic and regional defense plans for the first time since the Cold War.

C4ISR assets from NATO and national services will be an integral part of the NATO Force Model and support the requirements in the SASP and family of regional and subordinate strategic plans. C4ISR architecture and capabilities must also support a strengthened integrated air and missile defense (IAMD) through improved ISR for shared awareness, early warning, and tracking, and improved air and surface-based C2 systems. Persistent surveillance is needed to support the Alliance's I&W requirements. There will certainly be shortfalls in available assets and interoperability.

Strengthened IAMD is an important and new commitment associated with the 2022 Strategic Concept; it is a must to respond to the broad range of Russian air and missile capabilities, which can threaten allied populations, forces, and infrastructure from any direction given their ranges and mobility. Strengthened IAMD should include greater day zero connectivity and integration of existing IAMD-related C2 nodes, sensors, and effectors; new and improved IAMD capabilities; and an improved Air C2 system. The Air C2 system is already the focus of a transition effort by allies in conjunction with NCIA and ACO that seeks to address numerous shortfalls in the existing system while concurrently planning for the upgrades and development of an Air C2 system that can meet future needs. This transition effort should be accelerated. In particular, a strengthened IAMD should prioritize the ability to detect and defeat the broad range of tactical ballistic and cruise missiles in the current and future Russian inventory. This includes closing the low-altitude surveillance gap to detect and track cruise missiles across SACEUR's AOR.

Ongoing planning, force generation, and future exercises will identify C4ISR shortfalls and refine future C4ISR requirements to meet the demands of an improved NATO posture, including persistent surveillance and strengthened IAMD.

76 NATO, "New NATO Force Model," June 29, 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/220629-infographic-new-nato-force-model.pdf.

Robust, resilient, and integrated command structure and enhanced C2 arrangements.

NATO leaders recognize that the strengthened deterrence and defense posture they envision must be enabled by an improved Alliance C2 structure, parts of which do not yet exist. ACO's C2 structure currently includes one strategic headquarters (Supreme Headquarters Allied Powers Europe; SHAPE), three joint force commands (JFCs) (Brunssum, Naples, and Norfolk), three service component commands (Air, Maritime, and Land Commands), a theater logistics command (Joint Support and Enabling Command), and several operational commands (e.g., Striking Forces NATO, the NATO Airborne Early Warning and Control Force, and NATO Alliance Ground Surveillance Force).

The existing structure was designed for maximum flexibility and options to respond to multiple crises of different scale and operational requirements, primarily outside SACEUR's AOR. It was not optimized for collective defense. The JFCs do not have regional geographic boundaries or AORs. Maritime and Land Commands are neither manned nor trained for C2 of large-scale or AOR-wide operations. Staffs at strategic and operational levels lack critical expertise in key warfighting competencies (e.g., targeting, cyber defense and response, and space support).

Current ACO C2 structure and supporting command, control, communications, and computers (C4) systems (i.e., the current Air Command Control System, Federated Mission Network, Land tactical C2) are not yet fit for modern multi-domain warfare against a peer adversary. Viable Joint, Land, and Maritime C2 structures for an AOR-wide defense accommodating two new allies in the north (Finland and Sweden) will be priorities to establish. According to International Military Staff (IMS) Director of Plans and Capabilities Maj. Gen. Karl Ford, "SHAPE is working on a C2 assessment which will identify the drivers of change, review current capabilities and shortfalls, and propose design principles for future NATO C2."[77]

The assessment will look at C2 in three time horizons in order to capture short, medium, and long-term NATO adaptation needs. First, NATO C2 here and now and how to achieve the Concept for the Deterrence and Defense of the Euro-Atlantic Area (DDA) with the current NATO Command Structure and thirty allies. This stage aims to respond to current NATO needs, within the current membership format. Second, decision-makers are exploring NATO C2 needs for a potential thirty-two-nation Alliance, which would operate based on an MDO Concept and with a DT plan in place. This stage represents a much-expanded level of ambition, with NATO C2 over a contiguous northern region able to coordinate and execute cross-domain effects increasingly enabled by DT. Finally, the third stage will include SACT's vision of NATO C2 out to 2040 carrying out MDO and tailored to future challenges and threats that are expected to be increasingly persistent, boundless, and simultaneous from multiple state and non-state actors as well as from changes in the physical and social environment.[78] The third time horizon will be informed and enabled by the NATO Warfighting Capstone Concept (NWCC) and Warfare Development Agenda to get there.[79]

The NATO Force Structure must also be reviewed. This includes assessing requirements, overlaps, and gaps, in some cases rationalized (numbers of tactical headquarters), in some cases reinforced (creating sufficient manpower and expertise for MDO and peer combat), aligned with plans, and integrated with the NATO Command Structure (i.e., ACO and JFCs). The 2022 Strategic Concept's increased emphasis on resilience will require increased understanding and intelligence sharing of cyber and other related threats to civilian infrastructure. It will also require sustained investment to meet resilience targets (notably to improve cybersecurity and defense for NATO networks, national communications, transportation, health systems, and financial networks).

DT and increased cyber resilience will need to account for an enhanced NATO Command Structure integrated with a rationalized NATO Force Structure and connected to national forces associated with the new NATO Force Model and NATO plans.

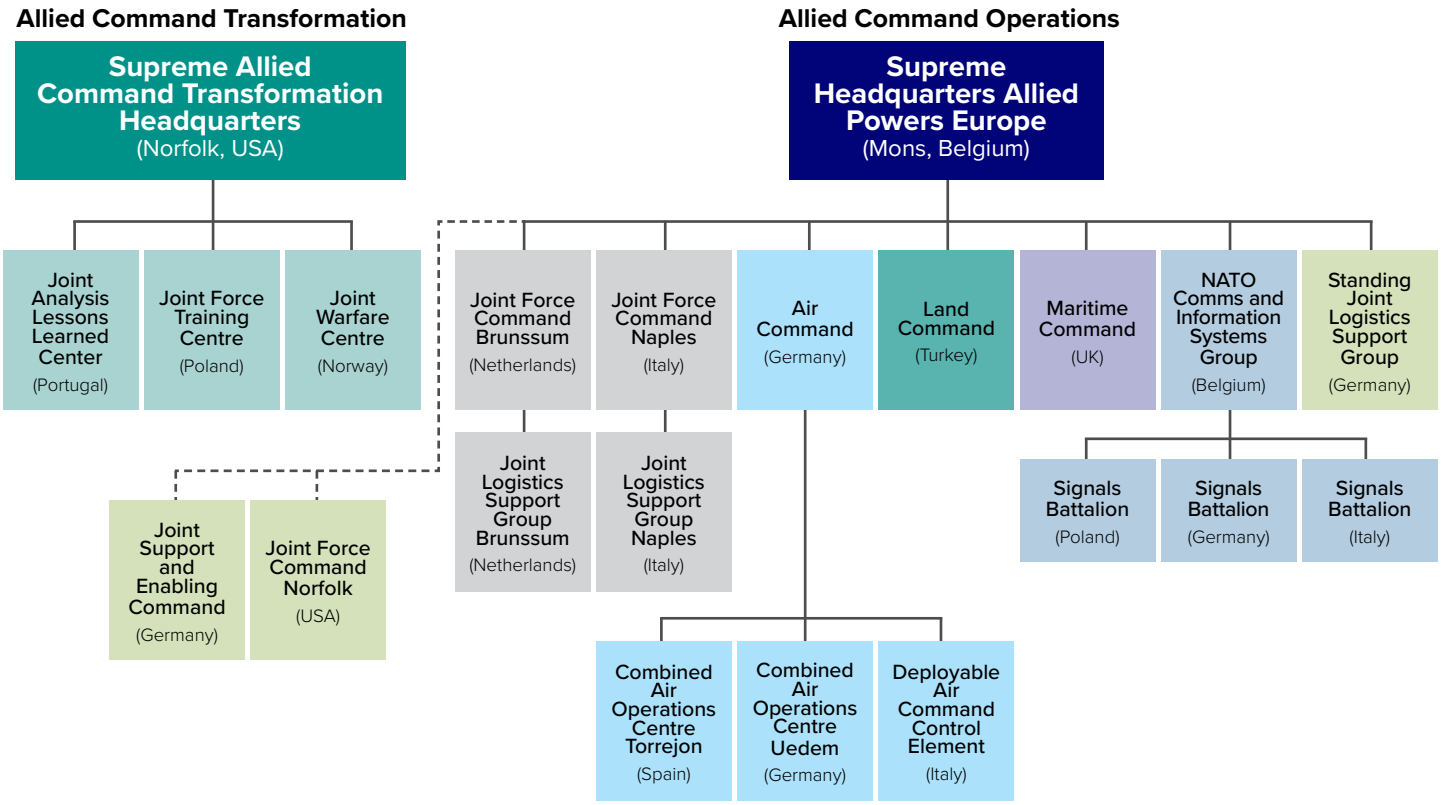
---

77 Maj. Gen. Karl Ford, interview by author, July 27, 2022.

78 Author's notes from unclassified ACT brief "2021 NATO Warfighting Capstone Concept" to the Conference of National Armaments Directors (CNAD) in Partner Format, NATO Headquarters, Brussels, January 29, 2021.

79 NATO, "The Alliance's Warfare Development Agenda: Achieving a 20-year Transformation," March 29, 2022, https://www.act.nato.int/articles/wda-achieving-20-year-transformation; Ford, interview.

Figure 3. NATO Command Structure



Credit: NATO.

Global awareness.

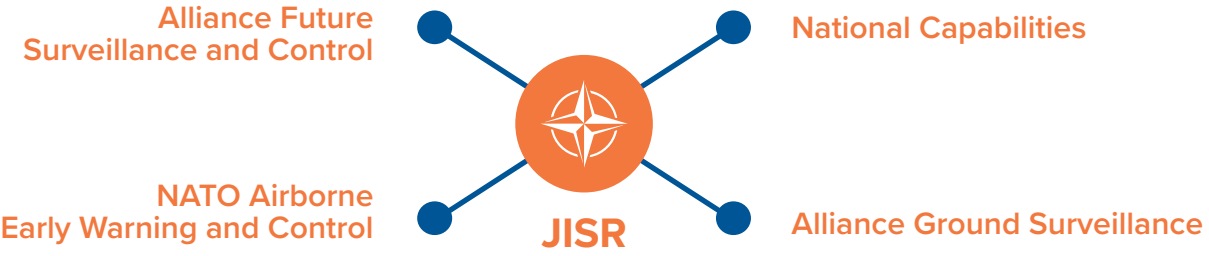
Enhanced shared, situational, and global awareness are all referenced in the 2022 Strategic Concept.[80] The first, enhanced shared awareness, implies improved collective awareness enabled by better intelligence sharing and more effective NATO C4ISR to enable timely and relevant intelligence for political and military leaders. The second, situational awareness, likewise implies timely and relevant intelligence and the addition of persistent surveillance of threat indicators that can rapidly evolve and thus require rapid response. The third, global awareness, refers to the need to monitor and analyze data and intelligence related to global factors such as climate change, pandemics, and strategic shocks emanating from abroad that could affect the Alliance. Global awareness also applies to China and Russia and their related activities and influence across the globe that impact Alliance security, interests, and values.

NATO's revised core tasks include deterrence by denial and crisis prevention. China and climate change are now characterized as long-term challenges. The revised tasks and long-term challenges will lead to new or revised strategic and operational intelligence requirements. Revised intelligence requirements will justify and generate a need for persistent, multidisciplinary, data-enabled, multi-domain NATO JISR and higher-quality and faster analysis to enable shared awareness, decision-making, and action at the speed of relevance (speed is more of a requirement for crisis and conflict than for long-term challenges).

Intelligence to enable awareness for crisis prevention and addressing long-term challenges will need to integrate inputs from a variety of national, regional, and organizational partners, and commercial providers (e.g., space industry, media, and data; computing; and network service and security providers). For example, broader NATO understanding of China would be enabled by financial, commercial, and science and

80 NATO 2022 Strategic, 5–7.

Figure 4. NATO's Joint Intelligence, Surveillance, and Reconnaissance (JISR) Concept



Credit: NATO.

technology data and analysis and greater information sharing with Indo-Pacific partners. NATO climate policy will require better analytics to understand and respond to the security implications of climate change and require greater NATO and national efforts to incorporate aspects of climate change mitigation in defense infrastructure and capability development (e.g., greater energy efficiency and use of sustainable energy sources, better monitoring of defense impacts on climate, reduced waste production, reduced carbon emissions, etc.).[81]

The approval of JISR Vision 2030+ by the North Atlantic Council (NAC) in Spring 2022 will enable enhanced awareness, multi-domain warfighting, and other aspects of the 2022 Strategic Concept. Giorgio Cioni, director of Armament and Aerospace Capabilities in NATO's Defense Investment Division, said the new JISR vision "includes a series of strategic outcomes, the overall purpose of which are to render JISR architecture more robust."[82]

Cioni said the strategic outcomes include: "1) increased investment in collection capabilities, looking beyond existing NATO-owned platforms and payloads (AGS and AWACS), achieving persistent surveillance through a combination of capabilities and services; 2) expanding the APSS initiative to collect and acquire space-based data, products, and services to improve NATO indicators & warnings and strategic anticipation; 3) improving PED [Processing, Exploitation, and Dissemination] with capabilities and tools to ensure timely and efficient analysis; 4) achieving coherence and integration of different programs contributing to the NATO C4ISR network of sensors, C2 nodes and systems, and effectors; 5) review of the JISR TCPED process to ensure it can cope with more data and capabilities (sensors, platforms, AI and ML tools) and support decentralized MDO operations; 6) enhance the human element of ISR, ensuring training and education of leaders, operators, intelligence professionals involved in ISR or end users of its output."[83]

NATO's level of ambition for global awareness will lead to much greater demands to provide persistent, multidisciplinary, data-enabled, and multi-domain NATO JISR. It will also instigate higher-quality and faster analysis which the new JISR Vision 2030+ and the existing JISR Capability Development Strategy should help NATO and its member states deliver.

Innovation and EDTs.

NATO is currently focused on protecting and fostering adoption of EDTs in "nine priority technology areas:" AI, data, autonomy, quantum-enabled technologies, biotechnology, hypersonic technologies, space, novel materials and manufacturing, and energy and propulsion.[84] The 2022 Strategic Concept states NATO's aims for innovation and EDTs.[85]

NATO has always focused on innovation as a critical element of maintaining its technological edge.

81 NATO, "Environment, Climate Change and Security," last updated July 26, 2022, https://www.nato.int/cps/en/natohq/topics_91048.htm.

82 Cioni, interview.

83 Ibid.

84 NATO, "NATO Sharpens."

85 NATO 2022 Strategic, 7.

However, since 2018 it has redoubled internal efforts to develop policy and external work to engage industry and the private sector to capture the potential of innovative technologies, concepts, applications, and processes.

Advanced, rapidly developing technologies have captured the attention of NATO leaders and led to a series of policies and plans related to EDTs. At the 2021 Brussels Summit, for example, NATO leaders agreed to stand up DIANA and a NATO Innovation Fund.[86]

According to Van Weel, NATO ASG for Emerging Security Challenges, the Alliance is learning how to promote innovation tailored to its needs. "We can create [a location and context to meet and discuss a particular topic], communicate what we want to achieve, and leverage civilian and commercial expertise," he said.[87] Van Weel also explained that for DIANA, "nations will collectively agree on strategic guidance developed from end users." The strategic guidance will include a set of prioritized defense needs developed by NATO Military Authorities (who set NATO defense requirements) and informed by the armaments community (consisting of the Conference of National Armaments Directors, or CNAD, and its subordinate structure, which are responsible for supporting capability delivery of NATO defense needs)[88] and the Science & Technology Organization (STO), which focuses on horizon scanning of technology developments and enabling collaboration in research and development (R&D).

This strategic guidance for DIANA will subsequently be transformed by the DIANA executive into challenge programs for the private sector. These challenge programs will articulate prioritized defense problems that will be shared with industry to seek potential solutions, much like how national security challenges are used by the US Defense Advanced Research Projects Agency to guide US government investment in private sector technology. NATO engagements to date have demonstrated that two-way communications with high-tech enterprises are more than just an opportunity for NATO to communicate needs.[89] This dialogue also exposes business opportunities that commercial enterprise may not know exist. "Many private sector companies don't know they can help in the defense and security field," said Van Weel.[90]

DIANA and the NATO Innovation Fund are being designed specifically to enable delivery of solutions versus simply to promote R&D. "DIANA will not just provide access to dual-use commercial solutions, but it will help mature them," said Van Weel. "Start-ups need founders, venture capital, business coaching, networking, and solution iteration between end users and industry. DIANA will make sure there is a connection with defense primes. The end of program is to showcase to all allies what solutions have been identified to respond to the agreed problems. Go to the Conference of National Armaments Directors, etc. And the NATO Innovation Fund can come in and put equity into a start-up company to help it scale up."[91]

NATO efforts to promote innovation and investment in EDTs will also help allies retain interoperability.[92] Interoperability by design is to be baked into capability development supported by DIANA and the NATO Innovation Fund. National efforts in R&D are less likely to be so inspired. Market competition and differing levels of available funding and technology across the Alliance will continue to create gaps in compatibility and interoperability. Without increased commitment by allies to ensure NATO interoperability as a requirement in the development of advanced technology, gaps will persist or increase.

Most of the nine priority technology areas that NATO EDT efforts are focused on will enable improvements in NATO C4ISR and consequently improve the speed and effectiveness of NATO intelligence, decision-making, and operational processes. Here are key

86 Brussels Summit Communiqué.

87 Van Weel, interview.

88 The CNAD and its seven Main Groups and over one hundred and fifty subordinate groups constitute NATO's largest standing committee structure and one of its longest standing. The CNAD is supported by NATO's DI Directorate. Collectively, the CNAD and DI Directorate are referred to as the NATO armaments community. See NATO, "Conference of National Armaments Directors (CNAD)," last updated January 17, 2023, https://www.nato.int/cps/en/natolive/topics_49160.htm.

89 NATO, "NATO Steps Up Engagement with Private Sector on Emerging Technologies," last updated September 15, 2022, https://www.nato.int/cps/en/natohq/news_207258.htm.

90 Van Weel, interview.

91 Ibid.

92 NATO 2022 Strategic, 7, par. 24.

points for four priority technology areas most relevant to NATO C4ISR:

1. **Expansion of AI and ML use cases and rapid adoption and scaling up of promising solutions will be critical for achieving NATO's ambition for C4ISR.** AI, ML, and Big Data services and tools have already been identified for their potential to enable future NATO C4ISR.[93] A few AI and ML use cases as described earlier are already underway (e.g., IEA's tool and NIFC's aircraft counting tool). These use cases are trials or proofs of principle to demonstrate that technology can improve speed and quality of output and provide new capabilities that respond to unmet needs.

2. **Autonomy promises cost-effective solutions across multiple domains which can increase endurance, reach, survivability, and performance of C4ISR in contested environments while reducing risk to operators.** Autonomy is a field of rapid development for NATO and involves land, maritime, and aerial systems.[94] It is significantly enabled by AI, ML, and Big Data services and tools. The NAGSF and future Alliance Future Surveillance and Control (AFSC)[95] are likely to be a subset of future aerial autonomous capabilities available to the Alliance. Land and maritime unmanned systems also promise great potential in delivering C4ISR capabilities. The NATO Maritime Unmanned Systems Initiative is a multinational effort and a splendid example of what collaboration between public and private sector approaches can achieve in terms of vision, capability development, and experimentation.[96] NATO's Project X (testing use cases for unmanned aircraft systems, or UAS, enabled by AI) is another excellent example of private-public collaboration and innovation.[97] Finally, countering adversary UAS capabilities is crucial for battlefield success as has been demonstrated in conflicts from the Middle East to Ukraine. C-UAS capabilities are a growing field of NATO collaboration with the private sector. NATO is testing C-UAS interoperability standards with both military and commercial capabilities.[98]

3. **Quantum technology in computers, communications, and sensors promises revolutionary changes for NATO C4ISR.**[99] Quantum computers will provide vastly improved processing speeds and capacity to enable data processing and exploitation to include decryption of current methods of secure communications. Quantum communications will enable improved security and unbreakable encryption. Quantum sensors will provide multispectral abilities to locate and identify objects previously undiscoverable due to cover and concealment,

Figure 5. NATO's nine priority technology areas

- AI
- Data
- Autonomy
- Quantum-enabled technologies
- Biotechnology
- Hypersonic technologies
- Space
- Novel materials and manufacturing
- Energy and propulsion

93 NATO Science & Technology Organization, *Science & Technology Trends 2020-2040*, March 2020, https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf.

94 Ibid.

95 NATO, "Alliance Future Surveillance and Control (AFSC)," https://www.nspa.nato.int/about/life-cycle-management/afsc.

96 Amir Husain and Michael D. Brasseur, "NATO's 'Startup' Is innovating in the Age of Exponentials, but Can It Scale?" *DefenseNews*, May 18, 2020, https://www.defensenews.com/opinion/commentary/2020/05/18/natos-startup-is-innovating-in-the-age-of-exponentials-but-can-it-scale.

97 Boeing, Boeing-NATO PROJECT X challenge spurs innovative ideas for future autonomous capabilities, press release, June 6, 2022, https://boeing.mediaroom.com/news-releases-statements?item=131059.

98 Caterina Tani, "SAPIENT – NATO's Future C-UAS Standard?" Mönch Publishing Group, accessed September 3, 2022, https://monch.com/sapient-natos-future-c-uas-standard/.

99 *Science & Technology Trends.*

including objects in buildings or underground and submarines under water. Of these three applications of quantum technology, NATO has already begun R&D projects and tests related to quantum communications.[100]

4. **Exponential increases in space-based capabilities over the coming decade will impact C4ISR requirements and resilience and enable C4ISR architecture and capabilities.** Space-related technology is included in EDTs, but managed under a distinct NATO Space Policy, which recognizes the role of national contributions from space-faring nations, but also unique NATO space support requirements (i.e., communications, intelligence, early warning, targeting, positioning, navigation, and timing).[101] NATO has had its own satellite communications capability for years, but in 2020 a group of allies contracted NCIA to expand its transmission capacity and improve the capabilities of NATO ground stations.[102] More recently, NATO has established a Space Center at ACO's Air Command (AIRCOM) in Germany,[103] a Space Situational Awareness Capability at NATO HQ,[104] and a Space Center of Excellence in France.[105]

Defense investment.

NATO's 2022 Strategic Concept mentions the importance of fulfilling the 2014 Defense Investment Pledge,[106] which was created to ensure adequate investment in defense in support of an ambitious NATO Readiness Action Plan[107] agreed at the 2014 Wales Summit.[108] The NATO Readiness Action Plan and increased defense investment were meant to adapt NATO politically and militarily in response to Russia's illegal annexation of Crimea earlier that year and its ongoing aggression against Ukraine. The pledge commits NATO allies to spend 2 percent of their gross domestic product (GDP) on defense by 2024 and to ensure 20 percent of defense spending is allocated for "major new equipment, including research and development."[109]

In the 2022 Strategic Concept, allies further commit "to provide the full range of required capabilities," "ensure that increased national defence expenditures and NATO common funding will be commensurate with the challenges of a more contested security order," and "increase our investments in emerging and disruptive technologies to retain our interoperability and military edge."[110] These new commitments are the sine qua non foundation for strengthening deterrence and defense and achieving the level of ambition NATO has set for adapting its political and military instruments of power to meet the threats and challenges of the coming decade.

NATO C4ISR structure and NATO-owned capabilities (e.g., AGS, AWACS, AFSC, JISR, Air C2 System, and Federated Mission Network) figure prominently in NATO's current defense investment programs and projects. Capability targets for national C4ISR are likely to increase in NATO's next defense planning cycle because of the new strategic environment and a new level of ambition to prepare for "high-intensity, multi-domain warfighting against nuclear-armed

100 NATO, "Using Quantum Technologies to Make Communications Secure," last updated September 27, 2022, https://www.nato.int/cps/en/natohq/news_207634.htm.

101 NATO, "NATO's Overarching Space Policy," last updated January 17, 2022, https://www.nato.int/cps/en/natohq/official_texts_190862.htm.

102 Brooks Tigner, "New Space Centres and Modernised Ground Sites to Support NATO Space Domain," *Janes*, October 21, 2020, https://www.janes.com/defence-news/news-detail/new-space-centres-and-modernised-ground-sites-to-support-nato-space-domain.

103 Supreme Headquarters Allied Powers Europe (SHAPE), "NATO Space Centre," accessed July 18, 2022, https://shape.nato.int/about/aco-capabilities2/nato-space-centre.

104 NATO, "NATO and Luxembourg Boost Alliance Space Situational Awareness," last updated June 15, 2021, https://www.nato.int/cps/en/natohq/news_185365.htm?selectedLocale=en.

105 Ministère de l'Europe et des Affaires Etrangères [France's Ministry of Europe and Foreign Affairs], "Defence – Establishment of the NATO Space Centre of Excellence in Toulouse – Communiqué issued by the Ministry for the Armed Forces," February 5, 2021, https://www.diplomatie.gouv.fr/en/french-foreign-policy/security-disarmament-and-non-proliferation/news/article/defence-establishment-of-the-nato-space-centre-of-excellence-in-toulouse; "NATO Space Centre of Excellence," accessed February 12, 2023, https://www.space-coe.org/.

106 NATO, "Funding NATO," last updated January 12, 2022, https://www.nato.int/cps/en/natohq/topics_67655.htm.

107 NATO, "Readiness Action Plan," last updated September 1, 2022, https://www.nato.int/cps/en/natohq/topics_119353.htm; NATO, "NATO Wales Summit Guide," Newport, September 4-5, 2014, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20141008_140108-summitguidewales2014-eng.pdf.

108 NATO, "NATO Wales Summit 2014," last updated September 5, 2014, https://www.nato.int/cps/en/natohq/events_112136.htm.

109 NATO, "Deterrence and Defence," last updated September 12, 2022, https://www.nato.int/cps/en/natohq/topics_133127.htm. See section on "Investing in defence."

110 NATO 2022 Strategic.

peer-competitors."[111] Both NATO-owned and national capabilities will consequentially be the object of future increases in defense spending.

In addition to supporting the costs of NATO's common military and civilian structure (i.e., manpower, operations, and sustainment), NATO common funding also supports collective defense investment in C4ISR capability development, which is of great political interest and subject to significant collective oversight and governance. Attempts to streamline and accelerate common-funded capability development and oversight have produced limited positive results to date. Low risk tolerance for early or any failure, detailed reporting requirements, and limited options for accelerated procurement are some of the main issues.[112] Upgrades of information technology (IT), which rapidly become obsolete, are taken as distinct collective decisions instead of being embedded in upfront requirements. Upgrades and modernization of major capabilities like NATO-owned AGS have been similarly delayed. Hence the need to review how NATO manages obsolescence in the modern age. The private sector provides ample examples of faster capability development and the NIAG has provided tailored advice on how to improve agility in acquisition.[113] Allies have not achieved the acceleration and expansion of common-funded capability development they desire, which has frustrated NATO military, civilian staff, and agencies involved. Further change is needed.

The NWCC, approved in 2021, managed by ACT, and supervised by the Allied Chiefs of Defense, should be a major driver of military innovation and investment over the coming decade, specifically concept and capability development.[114] While details in open sources are scarce, the NWCC will be managed through a Warfare Development Agenda that includes imperatives (e.g., cognitive superiority, multi-domain command, integrated multi-domain defense) and principles (e.g., right people, data centric technology, day zero integration, persistent disruptive preparation) which are meant to influence national and NATO C4ISR development and delivery decisions.[115] The ability to synchronize ACT's Warfare Development Agenda across NATO and nations and with existing NATO defense planning and capability development processes will be a daunting task. ACT has a direct role in common-funded capability development but has not yet leveraged its authorities and abilities to support national and multinational capability development.

DECISIONS TAKEN AT THE MADRID SUMMIT AND WORK UNDERWAY AFFECTING NATO C4ISR

- Multi-domain warfighting
- Digital Transformation
- Strengthened deterrence and defense posture
- Robust, resilient, and integrated command structure and enhanced C2 arrangements
- Global awareness
- Innovation and EDTs
- Defense investment

NATO ambition is high for its innovation and EDT adoption efforts, both of which are meant to direct investment into capability development that enables NATO's military edge. Initial efforts like DIANA, the NATO Innovation Fund, use cases for AI, and ongoing work to develop strategies for individual EDTs are all promising. Engagement with industry and the broader private sector is strong and growing. Similar to DT efforts, success in NATO innovation efforts will rely on an agility in investing in capability development and resource management

111 NATO 2022 Strategic, 6, par. 22.

112 Comments on NATO's common-funded capability development governance model and progress are based on the author's personal experience in NATO from 2018 to 2021. In 2018, a new governance model for common-funded capability development was adopted which was intended to empower NATO's strategic commands and agencies to drive capability development, introduce acceptable risk tolerance measures, streamline governance processes, and satisfy allies' appetite for control and cost-efficiency. Expected outcomes have been underwhelming. Learning has been steep, adaptation difficult, and control difficult for nations to release. The new governance model also controls common funding for IT and services (including cybersecurity), which require upgrades and modernization at speeds beyond which NATO processes can keep up.

113 NATO Industrial Advisory Group (NIAG), "Industry Initiative for Agile Acquisition (I2A2)," February 15, 2021.

114 Rear Admiral John W. Tammen, "NATO's Warfighting Capstone Concept: Anticipating the Changing Character of War," *NATO Review*, July 9, 2021, https://www.nato.int/docu/review/articles/2021/07/09/natos-warfighting-capstone-concept-anticipating-the-changing-character-of-war/index.html.

115 Ibid.

The importance of investing in NATO C4ISR innovation. Photo by NCI Agency.

(budgetary and human capital) that does not exist within NATO's current structure and processes. DIANA and the NATO Innovation Fund will offer alternative development and resourcing options to include bilateral, multilateral, and multinational programs. Scaling up solutions to provide NATO-wide enterprise capabilities would require common funding and be subject to NATO governance that has been historically resistant to higher risk and decentralized control. To achieve NATO's level of ambition, the Alliance will need to embrace a whole-of-enterprise effort, ensure sustained commitment and investment, and change the way it currently does business with regard to common-funded capabilities.

Deductions from the Madrid Summit and other recent developments include the following. NATO's 2022 Strategic Concept and recent policy decisions, including the political commitment to increase defense investment, have set the context for future NATO C4ISR. The foundation for future NATO C4ISR is being built through existing programs and initiatives, supporting concepts, assessments, and plans under development. The devil will be in the implementation of decisions taken and others still to be taken. The biggest challenges will be in achieving the cultural shift and sustained sense of purpose needed to enable a whole-of-enterprise approach in the face of inevitable resistance to change and competing domestic and global challenges.

RECOMMENDATIONS: SHARE, TRANSFORM, IMPLEMENT, MODERNIZE, AND INVEST

To maintain a comparative advantage against potential adversaries and challengers, NATO allies must

1) share more data and intelligence;
2) transform digitally;
3) implement new concepts, policies, and plans to clarify C4ISR requirements;
4) modernize, augment, and acquire capabilities to meet new C4ISR requirements; and
5) continue to invest in C4ISR interoperability, readiness, resilience, innovation, and adaptation.

Efforts are already underway to improve NATO C4ISR and more will follow as decisions taken at the Madrid Summit are implemented. Lessons and security implications from the Russia-Ukraine war for NATO C4ISR will and must be a priority for directing efforts and investment in C4ISR improvements, modernization, and future capability development. Due to its importance to effective Alliance security and defense, NATO C4ISR deserves special focus and effort to improve its multiple components (i.e., organizations, capabilities, networks, concepts, policies, processes, and people). NATO must change in several areas to maintain its technological and military edge and increase the likelihood of achieving the security and defense it deserves. The following recommendations build on positive momentum, leverage new concepts and initiatives, and offer suggestions for improvement, including adopting new efforts and approaches.

1. Share more data and intelligence.

Sharing data and intelligence is first and foremost a matter of political will, as NATO relies on voluntary information sharing by its allies. Sharing requires trust in NATO, specifically that the Alliance can protect information shared. Sharing will always be a delicate subject, as not all nations trust NATO or one another to protect their shared data and intelligence in the face of aggressive espionage, cyber incidents, mishandling, and leaks. NATO and its member states collect vast amounts of data and intelligence that are not exploited for the benefit of collective security and defense or other Alliance aims.

Trust is enabled by modern and secure networks, a common data framework and standards respected by all, and an efficient and effective NIE, all of which act as guarantees that the information can be protected and effectively exploited by the Alliance. Much of this is in place, but two key elements require attention: political will (greater emphasis) and security (continued emphasis).

The NAC must commit politically to addressing obstacles and shortfalls in sharing. Shared data or shared intelligence do not appear in the 2022 Strategic Concept or Madrid Summit Declaration. Their absence may reflect a view of adequacy in current levels of sharing or discomfort in addressing the many national policy and technical issues that affect trust in NATO's ability to protect data and intelligence.[116] Technical issues also inhibit interoperability, which must be addressed through greater emphasis on common standards (see sections 4 and 5 below). Shared data, information, and intelligence are fuel for C4ISR. Sharing is not at the level it can and needs to be to ensure NATO maintains its comparative military advantage.[117]

Security, including cybersecurity, remains an issue. But cybersecurity, document security, and communications security are improving with policy

116 NATO's first ASG for Joint Intelligence and Security (JIS), Arndt Freytag von Loringhoven, noted the "ingrained tradition" of national civilian intelligence agencies to restrict intelligence sharing in a 2019 article at the end of his tenure. See Arndt Freytag von Loringhoven, "A New Era for NATO Intelligence," *NATO Review,* October 29, 2019, https://www.nato.int/docu/review/articles/2019/10/29/a-new-era-for-nato-intelligence/index.html.

117 This is an uncomfortable truth acknowledged by current and past senior ACO intelligence officials (of which the author is one) and NATO's first two ASGs for JIS: David Cattler and Arndt Freytag von Loringhoven. Maj. Gen. Matt Van Wagenen, interview by author, September 11, 2022; Stewart, interview; Cattler, interview; and Von Loringhoven, "A New Era."

Officers analyze data coming in from the field at the trial control room during Unified Vision, NATO's main event for Joint Intelligence, Surveillance and Reconnaissance. Photo by NATO.

emphasis, cyber adaptation efforts, improved security measures, and with improved supporting tools being put in place or planned for the future.

A golden opportunity lies in the ability of NATO and its member states to tap into the potential of shared data and intelligence to exponentially improve the quality and speed of shared awareness, decision-making, and action. The opportunity cost of not sharing is enormous. For example, restricted sharing of intelligence on Russian violations of the Intermediate-Range Nuclear Forces (INF) Treaty complicated NATO consensus from 2014 to 2018 on US findings that the Russian 9M729 (or SSC-8) missile constituted a violation of the treaty.[118] Earlier sharing of sensitive intelligence could have significantly accelerated common positions on Russian nuclear-capable missiles, leading to earlier decisions on mitigation and pressure on Russia to comply. By contrast, the early decision by the United States and other NATO allies to share sensitive intelligence on Russian intentions vis-à-vis Ukraine in early 2022 led to greater and timely shared awareness, clarity in communications, and timely consensus on decisions taken to assure and defend allies and deter Russia.[119]

Here are basic, but critical, recommendations for NATO:

- **Implement the NATO Data Exploitation Framework Policy (DEFP) agreed by Alliance**

118 Despite numerous NATO consultations between 2014 and 2018 on the 9M729 or SSC-8 Russian missile (including when the author was an ACO presenter in 2014 and a NATO official in 2018), it was not until December 2018 that allies decided to unanimously endorse the US finding and presume the lack of an adequate Russian response as evidence of an Intermediate-Range Nuclear Forces (INF) Treaty violation. Several allies prior to late 2018 were not ready to take US declarations at face value without the primary source intelligence behind the US position. While the INF Treaty was between the United States and the Soviet Union, European allies were directly implicated because the treaty-limited ranges provided security from attack of prohibited weapon systems. See NATO, "NATO and the INF Treaty," last updated August 2, 2019, https://www.nato.int/cps/en/natohq/topics_166100.htm.

119 Stewart, interview; Cattler, interview; and Cioni, interview.

defense ministers in October 2021.[120] While details on the DEFP are not widely known, it is fundamental to establishing a common data framework across the NATO Enterprise to enable Big Data sharing, exchange, and exploitation. NATO Military Authorities (NMAs) have begun the implementation process, but it will require a whole-of-enterprise approach, with commitment from the nations, NATO HQ, and common funding. NCIA expertise and support will be critical. NATO should leverage the NIAG and look to industry for expertise and enabling services, such as cloud computing and Big Data management.

- **Task the NIE in conjunction with NMAs to assess and recommend critical improvements needed to enhance intelligence-sharing procedures and tools, specifically:**
  - Mutually supporting strategic and operational intelligence management procedures for warfighting and crises,
  - Intelligence functional services fit for MDO, and
  - AI tools to assist in real-time exploitation of shared intelligence (including sorting, cueing, and other automated functions).
- **Set realistic and measurable objectives to share more data with metadata, information, and intelligence, both military and commercial, related to threats and challenges.**

2. Transform digitally.

DT is a nascent effort that is fundamental for strengthening security and defense and improving resilience. DT is a key enabler of MDO. In turn, effective MDO depend on multi-domain C4ISR. Multi-domain C4ISR is critical for delivering multi-domain effects through multi-domain awareness, decision-making, and action. Enabling multi-domain C4ISR should, therefore, be a particular focus of DT.

A DT vision was developed in fall 2022 and an implementation plan is expected in 2023.[121] The 2021 DEFP is a fundamental first step in the process. The DT vision and implementation plan constitute policy that will have to be followed by investment in infrastructure, capabilities, people, supporting policies, and governance processes. Standards in data exchange and connectivity will be particularly important for networks, weapons systems, platforms, equipment, and software. The US Department of Defense's C4ISR/Electronic Warfare Modular Open Suite of Standards (CMOSS) provides a national example of an open standard approach that could be used to develop a similar NATO open standard approach allowing various national and commercial entities to design and develop interoperable capabilities.[122]

NATO DT must be comprehensive in its objectives and enterprise wide in its application to achieve what NATO needs for shared awareness, decision-making, and action at the speed of relevance for multi-domain warfighting as well as for effective crisis prevention and management.[123] NATO is politically committed to transform digitally, and policy development is in progress. As the NATO consultation, command, and control (C3) staff and board are central to DT policy development, implementation of DT into current and future C3 capability efforts is almost a given. A similar sense of urgency and focus will be needed across the NATO Enterprise. Given current positive momentum, NATO should:

- **Ensure funding matches political ambition** for and military (and Enterprise) requirements inherent to DT.
- **Ensure requirements** for enabling multi-domain C4ISR are captured, resourced, and addressed as a priority.
- **Seek and leverage private sector expertise and capabilities.** Large and small industries offer expertise and capabilities (services) related to DT.
- **Look long to enable transition to technologies and applications in NATO's near-term horizon** (i.e., the next six years), such as 6G networks and space-based capabilities and services.

120 Zoe Stanley-Lockman and Edward Hunter Christie, "An Artificial Intelligence Strategy for NATO," *NATO Review*, October 25, 2021, https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html.

121 Wheeler, interview and Criscuolo, interview.

122 Sally Cole, "CMOSS: Building-Block Architecture Bring Speed, Cost Benefits," Military Embedded Systems, November 29, 2021, https://militaryembedded.com/comms/communications/cmoss-building-block-architecture-brings-speed-cost-benefits.

123 The following Atlantic Council report explains the importance of enterprise-wide digitalization to improve shared awareness, decision-making, and action. Jeffrey Reynolds and Jeffrey Lightfoot, *Digitalize the Enterprise*, *Atlantic Council*, October 20, 2020, https://www.atlanticcouncil.org/content-series/nato20-2020/digitalize-the-enterprise/.

- **Ensure a whole-of-enterprise approach to link DT policy development and implementation**, including:
  - Active collaboration between relevant NATO governance bodies (e.g., those covering C3, cyber defense, security, armaments, standards, budgeting and resourcing, IAMD policy, defense planning) and the Military Committee, and
  - Collaboration within and among key staff management bodies (e.g., those responsible for communications, information and data management, cybersecurity, JISR, and innovation), including Strategic Commands, agencies, and perhaps Centers of Excellence where relevant.
- **Ensure the political focus and funding support to the NATO C3 community** to achieve and accelerate the delivery of critical C3 capabilities such as Federated Mission Network and Information Technology Modernization, and a standing operational net for current operations and activities (day zero readiness).
- **Ensure implementation of DT is integrated into related ongoing lines of effort beyond C3,** i.e., cyber defense adaptation, standards development, common-funded capability development, multinational capability development cooperation, and complex armaments programs (e.g., Air C2, AWACS, and AFSC).
- **Adapt existing service contracts and capability development plans, programs, and project**s to include DT implementation guidance and standards.
- **Develop and implement a human capital development and management policy** focused on hiring the right talent, and training and educating NATO civilian and military workforce and leaders to enable DT. Seek and leverage private sector expertise.

3. Implement new concepts, policies, and plans to clarify requirements for NATO C4ISR.

NMAs determine C4ISR requirements through the NATO defense planning process (NDPP), and the NAC and allies decide how to meet those requirements through collective, multinational, and national capabilities. NATO's C3 community plays a key role in determining the technical aspects of interoperable and secure C2, communications, and computers for NATO's military and broader NATO Enterprise. With this as context, several efforts underway over the next year or the longer term will directly influence future NATO C4ISR requirements. The Alliance should leverage these efforts to clarify requirements and ensure coherence in the next NDPP cycle and future capability development and delivery to develop the future C4ISR architecture NATO needs.

First, the new NATO Force Model and alignment of forces with NATO's new family of plans (SASP and regional and subordinate strategic plans) will identify C4ISR force and capability requirements. This effort is underway and will likely conclude at the June 2023 defense ministers' meeting.[124] These requirements could include new or revised NATO C4ISR structure. If force generation shortfalls reflect shortfalls in national inventories, then C4ISR capability requirements should increase.

Second, an Alliance MDO Concept will help define what NATO C4ISR must deliver to outthink and outpace potential adversaries and how NATO C4ISR will contribute to achieving multi-domain effects. The final Alliance MDO Concept is under development by the Strategic Commands and allies expect it to be delivered in 2023. Likewise, a DT implementation plan is expected in the first half of 2023.[125] DT is a fundamental condition for MDO and will set standards for digitalization, connectivity, and data exchange and exploitation that will affect current and future NATO C4ISR.

Third, NATO leaders have tasked ACO to produce a C2 Assessment to enable allied ministers to consider new requirements from NMAs and defense policy proposals (from relevant committees) by Spring 2023.[126] Adjustments to the NATO Command

124 Ford, interview.

125 Criscuolo, interview.

126 Ford, interview.

Structure over several time horizons will impact C4ISR requirements, specifically to enable effective AOR-wide C2 and multi-domain warfighting. The NATO Force Structure, which is composed of allied national and multinational forces and HQs, should also be part of proposals for change to execute SASP and support the new NATO Force Model. Additional or new C4ISR structure should be considered as well. The timing of the ministers' decision in 2023 is fortuitous and will allow endorsed C4ISR-related requirements to be captured in the next NDPP cycle, specifically in the Minimum Capability Requirements (MCR) that NMAs will produce for NAC approval in 2024.

Fourth, over a longer term, the JISR component of NATO C4ISR is driven by several agreed documents and programs. Strategic outcomes of NATO's JISR Vision 2030+, discussed earlier along with the JISR Capability Development Strategy, and JISR community stakeholder decisions will drive enhancements in JISR capabilities, including existing JISR programs and initiatives (e.g., AGS, APSS). JISR Vision 2030+ strategic outcomes will address NATO TCPED (structure, tools, and processes), human capital supporting JISR architecture, and overall coherence in JISR architecture.[127]

There is another effort not yet on NATO's task list that merits attention. A clarifying definition for NATO C4ISR does not exist (as a whole versus in its subcomponents of C2, C3, or C4, and JISR). NATO Architecture Framework Version 4 provides guidance for developing, designing, and managing enterprise architectures.[128] According to Paul Savereux, director of Defense Planning in NATO's Defense Policy and Planning Division, NATO C4ISR capabilities are addressed in multiple planning domains of the NDPP but are neither aggregated nor treated as part of a single function.[129]

Achieving the full potential of NATO C4ISR and ensuring it is fit for multi-domain warfighting requires coherence in defense planning, capability, and concept development supported by a recognized and defined NATO C4ISR architecture. A defined C4ISR architecture would harmonize defense planning efforts across multiple domains, enable aggregation and assessment of related capability targets, and ensure greater coherence in concept and capability development. A common definition would assist in the development of common standards for the various components that comprise or enable C4ISR (including interfaces and data-sharing protocols).[130] A common definition would also enable engagement with the private sector.

Here are some recommendations for NATO to capitalize on current efforts and improve their collective outcomes relative to C4ISR. NATO should:

- **Define NATO C4ISR architecture to provide a shared understanding of what makes up NATO C4ISR** in terms of capabilities (forces, systems, platforms, networks, applications) and enabling policies, concepts, standards, and processes.
  - Author's proposed definition: NATO C4ISR architecture is the whole of structures, organizations, systems, platforms, networks, applications, policies, concepts, and processes connecting decision-makers, operators, intelligence professionals, and capabilities in support of NATO shared awareness, decision-making, and execution in a multi-domain environment.
- **Include goals or objectives and operating principles for each of the key NATO-owned components of NATO C4ISR architecture that leverages existing elements and addresses gaps.** This would allow for a methodical approach to determining effectiveness and progress over time of both components of NATO C4ISR and C4ISR architecture as a whole.
- **Ensure C4ISR requirements are rigorously collected from efforts to strengthen deterrence and defense** through the NATO Force Model aligned with the SASP and family of plans, to conduct MDO, to digitally transform NATO, and to enhance C2.

---

127 Per AJP-2.7, JISR architecture consists of the organizations, processes, and systems connecting collectors, databases, applications, producers, and consumers of intelligence and operational data in a joint environment. See NATO Standardization Office, *NATO Standard, AJP 2.7, Allied Joint Doctrine for Joint Intelligence, Surveillance and Reconnaissance, Edition A, Version 1,* July 11, 2016, 1–3, https://jadl.act.nato.int/ILIAS/data/testclient/lm_data/lm_152845/Linear/JISR04222102/sharedFiles/AJP27.pdf.

128 Architecture Capability Team, Consultation, Command & Control Board, *NATO Architecture Framework, Version 4*, NATO, January 2018, Document Version 2020.09, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/1/pdf/NAFv4_2020.09.pdf.

129 Paul Savereux, interview by author, July 29, 2022, and NATO, "NATO Defence Planning Process," last updated March 31, 2022, https://www.nato.int/cps/en/natohq/topics_49202.htm.

130 Fabrice Fontanier, chair of NIAG C4ISR Community of Interest, notes to author, September 17, 2022.

- **Improvement of the TCPED process (a strategic outcome of JISR Vision 2030+)** should be an early focus of DT and EDT efforts (e.g., related to AI, data, autonomy, and space) to enable speed and multidisciplinary intelligence fusion, and improvements in processing capacity and quality demanded for multi-domain warfighting.
- **Leverage existing NATO C4ISR forces and build upon their potential.** Consider adjustments to NATO C4ISR forces (NAEW&CF and NAGSF) to enhance their effectiveness and contributions in support of the SASP and force generation related to the NATO Force Model.[131]
  - The NAEW&CF has two subordinate component commands, one of which (the British national component) is currently phasing out its E3Ds for higher performance E7s. The NAEW&CF could potentially command other nationally contributed C4ISR platforms or new NATO C4ISR forces. Similarly, the NAGSF has the potential to command additional JISR assets and platforms.
  - NATO should review NAEW&CF and NAGSF manpower and operational requirements, and funding levels for operations and sustainment to support a higher level of baseline activities and missions in view of the new political ambition for strengthened deterrence and defense.
- **NATO should ensure C4ISR coherence throughout the defense planning process.**
  - C4ISR elements contained in *Political Guidance 2023* should be mapped and consolidated for future reference, e.g., through the delivery of MCR in 2024.
  - C4ISR-related MCR should be the subject of multi-domain wargaming based on the SASP, the NATO Force Model, ACO C2 adjustments, and known NATO capability program milestones.
  - NATO should ensure a method to aggregate and track C4ISR-related capability targets apportioned in 2025.
  - Revised procedures for capturing C4ISR requirements will also enable biennial assessments of progress in achieving C4ISR-related targets.

4. Modernize, augment, and acquire capabilities to meet new C4ISR requirements.

This category of recommendations is the most extensive and associated with practical delivery of what the Alliance needs to maintain its technological edge and comparative military advantage over the coming decade. The following recommendations are grouped by central themes.

(A) The first step must be ensuring coherence in concept and capability development. Such coherence does not yet exist. A recognized definition for NATO C4ISR architecture will help, but other steps must be taken to ensure 1) a whole-of-enterprise approach, 2) synergy between political and military efforts, and 3) greater agility and effectiveness in concept and capability development.

- **NATO must take a holistic approach to C4ISR concept and capability development.** Cross-committee efforts related to C4ISR policy and capability development need a forcing function, including top-down guidance with clear responsibilities for lead, but also NATO Enterprise contribution to ensure coherence and synergy. NATO committee and military efforts supporting concept and capability development must be better connected and integrated.
  - Implementation of ACT's Warfare Development Agenda should incorporate a coherent approach to C4ISR concept and capability development, enabled by a defined NATO C4ISR architecture.
  - The approach intended for DT (modernize, optimize, transform concurrently) is practical and inherently agile and offers an example of how C4ISR capabilities can be planned and developed in concurrent phases.

(B) According to NATO Deputy ASG for Defense Investment Robert Weaver, on October 2021 the CNAD agreed a NATO armaments policy on Achieving and Accelerating Capability Development and Delivery (A2CD2).[132] Speed, agility, and effectiveness are at the heart of this policy, which aims to identify opportunities for accelerated delivery, pursue approaches with highest potential payoffs, and

131 A JAPCC NATO ISTAR white paper offers a recommendation for a NATO ISTAR structure based on augmenting the NAGSF. See Col. Maurizio De Angelis et al., "Chapter 9 - Future C2 for NATO-Owned ISTAR" in *NATO ISTAR - Establishing a NATO-Owned Intelligence, Surveillance, Target Acquisition, and Reconnaissance Capability*, JAPCC, February 2022.

132 Robert Weaver, interview by author, March 11, 2022.

A soldier sits inside a Boeing AWACS reconnaissance plane. Photo by Johanna Geron via REUTERS.

deliver results. Greater collaboration between the CNAD, Science & Technology Board, and Strategic Commands is the primary enabler of the policy's aims. The policy includes ideas for increased multinational cooperation, leveraging testing and experimentation within NATO exercises to enable warfighter interaction with the private sector, wargaming and tabletop exercising of capability solutions, and improved collaboration in concept development.[133]

ACT and ACO need to change how they currently support capability development to enable A2CD2 policy implementation. ACT currently focuses primarily on common-funded capability development and experimentation and lower technology readiness levels, which limits support to other approaches to capability development (i.e., national and multinational). ACO owns control, design, and funding of training and exercises, which offer the venue and opportunity for critical testing and experimentation of maturing technologies. However, ACO has ceded responsibility for operational testing and experimentation to ACT along with capability integration.

- **NATO leaders should encourage NMAs to take a broader role in supporting national and multinational capability development** through operational experimentation efforts. NATO should ensure both authority and funding to do so.
- **NATO leaders should align appropriate responsibilities and focus within the Strategic Commands concerning operational testing and experimentation.** Testing and experimentation opportunities are critical for enabling warfighter interaction with industry. They lead to industry refinements necessary for effective capability delivery. They also lead to warfighter awareness of new technology and applications and follow-on action to develop the concepts, plans, and procedures for effective integration. ACO Maritime Command's collaboration with ACT, nations, and private industry in preparation for

133 Ibid.

exercise Dynamic Messenger in September 2022 is a good example of operational testing and experimentation that deserves replication and institutionalization.[134]

- **NATO leaders should expand and ensure dedicated funding for biannual Unified Vision trials** (long-standing ACO interoperability tests and experimentation supported by ACT, nations, and the JISR community) to include testing and experimentation of mature promising C4ISR capabilities and enablers.

(C) Modernize, augment, and build on existing C4ISR force structure. NATO's AFSC program's innovative approach of partnering closely with industry to replace AWACS by 2035 with C4ISR capabilities that are fit for the future offers an excellent example of innovation in action.

At the Madrid Summit, NATO leaders expressed their commitment to support the AFSC program into design and delivery and procure an advanced C4ISR platform in time for crew training to replace NATO E3As as they start to phase out in the early 2030s. "The fast-track approach will deliver an initial element of the AFSC capability in coherence with the agreed AFSC concept and with the subsequent stages of delivery of the selected technical solution," said Cioni, director of Armament and Aerospace Capabilities in NATO's Defense Investment Division.[135] The selected technical solution is yet to be determined and may consist of crewed and/or unmanned systems or a network of systems. Follow-through with political commitment and funding over the life of the AFSC program will be critical.

NAEW&CF and NAGSF have the potential to deliver more and to satisfy new requirements related to strengthened deterrence and defense. With respect to the NAGSF, NATO needs more platforms and sensor capabilities (such as IMINT/FMV/EO/IR and SIGINT) to enable effective support to its core tasks.

- **NATO should integrate national contributions** on a permanent or rotational basis into the NAEW&CF and NAGSF based on NATO Force Model force generation to meet C4ISR requirements within NATO plans.
- **NATO should authorize and provide the funds for NAEW&CF and NAGSF commanders to leverage AI, ML, and Big Data** management and exploitation tools. Such adoption must be in line with DT principles but will exploit the vast opportunities for improving image or signals recognition and classification, database management, maintenance, and planning for NAEW&CF and NAGSF. Such tools could also enable a sense and avoid capability for AGS.
- **NATO should upgrade, augment, resource, and fully exploit the NAGSF.** The NAGSF has been effective and responsive but is still at Initial Operational Capability. NATO and nations should:
  - Fund and accelerate infrastructure. Provide the required manpower to achieve Full Operational Capability.
  - Fully leverage the analyst and operator training provided by the NAGSF.
  - Fully leverage the NAGSF's PED potential through full manning and rotation of national analysts as members or augmentees. Experience in the NAGSF provides an opportunity for national analysts to gain expertise for national employment and contribute to NATO intelligence requirements.[136]
  - Fund the validated critical modernizations and upgrades required for current operations (especially Link 16, a standardized communications system used by the US military and its NATO allies, and secure communications accreditation).
  - Plan now and fund the acquisition of sensors (IMINT and SIGINT) to upgrade AGS platforms and fill gaps in collection capability.
  - Plan early to replace AGS RQ-4s at the end of their operational life span.
- **Fully fund AFSC development, including the fast-track approach**, to ensure seamless delivery of the advanced C4ISR capabilities NATO needs for multi-domain warfighting beyond 2030.

134 NATO, "NATO Exercises with New Maritime Unmanned Systems," last updated September 15, 2022, https://www.nato.int/cps/en/natohq/news_207293.htm.

135 Ibid.

136 Stewart, interview and Cantwell, interview.

(D) APSS needs political commitment and funding and deserves expansion. NATO-owned JISR platforms provide IMINT and measurement and signature intelligence (MASINT).[137] NATO exploits significant amounts of OSINT to include commercial satellite imagery. The APSS initiative will significantly enhance the ability to receive national and commercial space-based information (imagery, signals, electronic signatures). NATO relies on nations for a greater breadth of IMINT as well as SIGINT, human intelligence (HUMINT), and cyber intelligence (multi-source). Multi-discipline intelligence fusion is critical for confidence in the analysis that enables shared awareness, consensus decision-making, and action. Additional IMINT and SIGINT capabilities (NATO-owned or contributed by nations) are needed now and offer promising prospects for improving NATO C4ISR. NATO should:

- **Expand its APSS initiative to include all allies.** In support of APSS, NATO should:
  - Encourage national contributions and funding to meet strategic and operational intelligence requirements.
  - Limit bureaucracy by keeping governance simple and lean, ideally supported by existing committee structure.
  - Enable the NIE to fully exploit the multiple intelligence disciplines that space-based assets offer.
  - Consider including national and commercial high-altitude platforms (balloons, airships, aircraft that operate in the stratosphere) that can contribute to persistent surveillance.
- **Ensure space data collection, exchange, and exploitation requirements** are part of DT.
- **Ensure the space expertise required to exploit space-based C4ISR capabilities is established** within the Strategic Commands (ACO and ACT).
- **Integrate IMINT and SIGINT capabilities into NATO C4ISR** (multiple options—additional sensor payloads for existing platforms, national contributions augmenting existing forces, and new platforms with IMINT and SIGINT sensor payloads).
- **Develop and implement policy to normalize and integrate SIGINT** (military and commercial) for operational and tactical use across NATO Command and Force Structures.

(E) Integration of NATO air and missile defense requires additional efforts to close gaps in sensors, Air C2, Ground C2, and Tactical Data Links (TDLs) between sensors, weapons, and C2 platforms. NATO IAMD requires a special focus due to its critical role in protection of NATO C2, forces, and populations. NATO IAMD relies on C4ISR capabilities to ensure operational sensing, decision-making, and action. The ground-based air defense (GBAD) C2 multinational cooperation project supported by the CNAD promises focused solutions to integrating disparate allied GBAD C2 systems at the brigade and battalion level.[138]

A similar effort is needed to integrate Surface-Based Air and Missile Defense (SBAMD includes land and maritime systems) for area defense of NATO critical assets. NATO TDL standards are particularly important for NATO IAMD, yet not completely implemented by nations.[139] Select air and missile defense platforms (i.e., fifth-generation aircraft) are becoming more advanced and capable of serving simultaneously as sensors, C2 nodes, and effectors. Yet these advanced platforms cannot seamlessly share tactical data. NATO and national investment in TDL software and hardware is critical. Additional R&D is required for data sharing between fifth-generation aircraft. NATO should:

- **Connect existing ground radars and field additional surface or space-based sensors required across the Alliance** to close the radar sensor gap for low-flying threats (below 5,000 feet).
- **Develop a NATO program for the network of sensors and C2 nodes** needed to ensure shared early warning, tracking, and engagement of hypersonic threats.

137 NATO's AGS RQ-4Ds are equipped with MP-RTIP ground surveillance radar that provides ground moving target indicator and synthetic aperture radar imagery. See Wikipedia, "Multi-Platform Radar Technology Insertion Program," accessed July 29, 2022, https://en.wikipedia.org/wiki/Multi-Platform_Radar_Technology_Insertion_Program#Overview. NATO's AWACS E-3s have look-down radar that essentially collects MASINT. See "E-3 AWACS."

138 NATO, "Command and Control Capability for Surface Based Air and Missile Defence for the Battalion and Brigade Level (GBAD C2 Layer)," Factsheet, February 2022, https://www.nato.int/nato_static_fl2014/assets/pdf/2021/10/pdf/2110-factsheet-gbad-c2-layer.pdf.

139 Military Wiki, "Tactical Data Link," accessed September 1, 2022 https://military-history.fandom.com/wiki/Tactical_Data_Link#TDL_standards_in_NATO.

NATO Cyber Security Centre. Photo by NCI Agency.

- **Accelerate transition to a future Air C2 system** fit for multi-domain warfighting and future threat and friendly capabilities.
- **Focus innovation and capability development efforts on integrating sensors, C2, and effectors at the higher tactical (above brigade) level and AOR wide.**
  - NATO needs political commitment and national action to ensure its TDL standards are implemented in national and NATO platforms.
  - Nations must follow through with integration of Link 16 capability in appropriate land, maritime, and aerial platforms.
  - NATO needs to prioritize Link 16 capability for the NAGSF in its modernization and upgrade efforts.
  - Nations must follow through with integration of Link 22 in maritime systems to replace Link 11, ensure Link 16 compatibility, and improve overall interoperability.
  - The United States needs to accelerate development of an interoperable TDL network between its fifth-generation aircraft and compatible with NATO TDLs.[140]

(F) EW capabilities are central to modern warfare and a principal focus of peer adversaries due to their potential for asymmetric response to Alliance comparative advantages (i.e., high-performance C4ISR platforms, precision-guided missiles). EW capabilities support intelligence collection and targeting, disrupt or destroy C4ISR, and require specialized C2 for effective employment. EW offensive capabilities can be relatively low-cost and range from radars to jammers to direct energy weapons to missiles guided by electromagnetic (EM) seekers.

140 Harry Lye, "Fifth-Generation Aircraft Share Bi-Directional Data in Military IoT First," *Airforce Technology*, December 15, 2020, https://www.airforce-technology.com/news/fifth-generation-aircraft-share-bi-directional-data-in-military-iot-first/.

Protection from adversary offensive EW capabilities is critical for NATO C4ISR. NATO operational and tactical communication networks must be secure, survivable, and resilient in a contested environment. Low probability of intercept, low probability of detection, directional communications, and autonomous functions can support improved security, survivability, and resilience.[141] Self-organizing networks should be the aim with autonomous functions supported by AI and next generation network capabilities (i.e., 5G, 6G) and may require new waveforms enabled by new radio and antenna systems.[142]

The NATO EW community is active in promoting policy, doctrine, and capability development, but has not gained the political attention and commitment needed to ensure development of NATO EW capabilities to the level needed for modern warfare.[143] NATO's Joint Airpower Competence Center (JAPCC) has developed several recommendations for NATO action related to EW that could enhance NATO C4ISR effectiveness.[144] Building on JAPCC's recommendations NATO should:

- **Establish a Strategic EW Operations Center** to enable NATO C2 of and employment guidance for nationally contributed EW capabilities and assets and assist in doctrine and concept development and training.[145]
- **Ensure modern warfare EW capability needs are prioritized in NATO defense planning.** Specifically include a focused section in *Political Guidance 2023* and ensure the development of appropriate MCR in 2024 (leveraging modern warfare lessons and ambitious wargaming).
- **Promote national and multinational capability development and delivery of prioritized EW capabilities** that improve security, survivability, and resilience of C4ISR, including through NATO innovation initiatives.
- **Integrate EM operations in the Alliance MDO Concept and clarify policy and doctrine** on how the electromagnetic spectrum (EMS) fits into existing operational domains. (For example, should the EMS be merged into a single cyberspace-EMS domain?)[146]
- **Develop a culture of EM signature awareness among all forces** (especially land forces) and integrate EM signature monitoring, control, and mitigation into all (including C4ISR) new systems and capabilities.

(G) NATO recognizes the importance of investing in and promoting innovation and adoption of EDTs to retain its "technological and military edge."147 The DIANA and NATO Innovation Fund initiatives as explained earlier provide great promise in developing the "innovation ecosystem" and collaboration with private sector that is needed to identify, promote, and deliver solutions to NATO's operational and business challenges.[148] DIANA will focus on leveraging innovation and creative solutions from start-ups and SMEs, but will include the NIAG throughout its processes to ensure wider industry awareness and preparation of defense and aerospace primes for scaling up promising solutions when necessary.

Complementary efforts are needed in three areas to leverage the potential that innovation and EDTs offer. First, clarification of the role of NATO's military in innovation could empower NMAs to focus on improving the quality and substance of their collective contributions, including NATO Enterprise-wide collaboration. Second, greater agility in common-funded capability development and resourcing is needed to modernize how NATO acquires C4ISR capabilities and services. Third, NCIA as a customer-funded agency should be leveraged by allies to

141 Fontanier, notes to author.

142 Ibid.

143 Commander Malte von Spreckelsen, "Electronic Warfare – The Forgotten Discipline," *Journal of the JAPCC* 27 (2018), 41–45, https://www.japcc.org/articles/electronic-warfare-the-forgotten-discipline/.

144 De Angelis et al., *NATO ISTAR*, 52; Von Spreckelsen, "Electronic Warfare"; and Major Erik Bamford and Commander Malte von Spreckelsen, "Future Command and Control of Electronic Warfare," *Journal of the JAPCC* 28 (2019), 60–66, https://www.japcc.org/articles/future-command-and-control-of-electronic-warfare/

145 De Angelis et al., *NATO ISTAR*, 52.

146 Colonel Matthew Willis and Lieutenant Colonel Panagiotis Stathopoulos, "Cyber-Electromagnetic Domain," *Journal of the JAPCC* 30 (2020), 72–77, https://www.japcc.org/wp-content/uploads/JAPCC_J30_screen.pdf.

147 NATO 2022 Strategic, 7.

148 Van Weel, interview.

provide greater support to national and multinational capabilities and services related to C4ISR.[149] NATO should:

- **Formalize and improve contributions from NATO's military to innovation.**[150] Elements of which follow:
  - NWCC includes future capability considerations that should be refined over time through dialogue with the Armaments Community and STO.
  - The Warfare Development Agenda is meant to drive concept development and influence capability development but must be aligned with the NDPP.
  - Military requirements can be better informed by engagement with industry, the Armaments Community, and the Science & Technology Board.
  - Promotion of innovation challenges to military problem sets should be developed through greater involvement with the NATO Enterprise.
  - Military advice and input into the strategic guidance for DIANA are critical for leveraging DIANA's potential to address military problems and challenges.
  - Support for testing and experimentation (including warfighter-industry interaction) of maturing technology and applications in NATO training and exercises needs greater focus.
  - Concept development is not yet at pace to leverage maturing technology and applications to enable integration and effective employment.
- **Adopt agile capability development and resourcing principles for common-funded C4ISR capabilities and services.**
  - Revise how IT components of capabilities are addressed in requirements and acquisition to account ahead of time for cybersecurity, obsolescence replacement, upgrades, and modernization.
  - Reduce complexity in requirements drafting and committee oversight but enforce schedules.
  - Adopt modular approaches to design to enable interchangeability and interoperability among capabilities.
  - Adopt advanced technology that is mature, available, and corresponds to need rapidly.
  - Allow for an approach that includes early prototype testing and experimentation, small-scale purchases, building on success, and scaling up.
  - Allow for the appropriate risk tolerance for failure and revision.
- **Fully leverage NCIA's potential support to national and multinational capability development and services related to C4ISR.** Recent contracts for satellite communications, Strategic Space Situational Awareness System, and APSS are great examples of NCIA's ability to leverage funding from single allies and groups of allies to provide capabilities and services that benefit the entire Alliance.

5. Continue to invest in NATO C4ISR interoperability, readiness, resilience, innovation, and adaptation.

NATO's value added to allies are its abilities to collectively decide and act, organize, and integrate. NATO provides the structural and digital backbone for nations to plug into, and develops common doctrine, concepts, procedures, and capabilities to enable interoperability and effective collective action. NATO nations have already increased defense spending by the equivalent of $350 billion since making their Defense Investment Pledge in 2014.[151] More billions of dollars are planned to be spent by 2024 and beyond as additional allies meet or exceed their defense spending goal of 2 percent of their GDP. As of June 30, 2022, eight allies exceed the 2 percent goal.[152] A total of nineteen allies have plans to do so

149 NATO Support and Procurement Agency (NSPA) is already involved in major C4ISR programs like AFSC, AWACS, and AGS. NCIA focuses almost overwhelmingly on common-funded capabilities and services but could provide support to multinational and national capability development given its charter and expertise.

150 Based on ideas discussed between the author and Lt. Gen. Hans-Werner Wiermann in February 2021.

151 NATO, "Remarks by NATO Secretary General Jens Stoltenberg and US President Joe Biden at the start of the 2022 NATO Summit," last updated June 29, 2022, https://www.nato.int/cps/en/natohq/opinions_197374.htm.

152 Katharina Buchholz, "Where NATO Defense Expenditure Stands in 2022 [Infographic]," *Forbes*, June 30, 2022, https://www.forbes.com/sites/katharinabuchholz/2022/06/30/where-nato-defense-expenditure-stands-in-2022-infographic.

by 2024 and five more plan to meet the goal shortly after 2024.[153]

NATO-owned C4ISR forces (e.g., NAEW&CF and NAGSF) and capabilities ensure a guaranteed minimum level of shared data and intelligence that is rapidly employable to enable political and military shared awareness. NATO-owned assets have proven their value time and again in crisis and partially compensate for the lack of standing national C4ISR contributions. The C4 elements of NATO-owned C4ISR assets provide secure and interoperable C2 and secure computer and communications networks for political consultation and NATO military operations and activities (strategic to tactical).

NATO-owned C4ISR forces and capabilities are NATO's added value to the Alliance, providing the interoperable structure and digital backbone into which national contributions plug for collective awareness, decision-making, and action. Investment in NATO-owned C4ISR forces and capabilities can only enhance the Alliance's capability to observe, orient, decide, and act.

NATO C4ISR will reap the benefits of known and expected increases in defense spending. While the bulk of allied defense spending will go to national defense requirements, spending on increased readiness of national C4ISR forces (personnel, training, equipment, sustainment, and infrastructure), enhanced resilience (especially communications networks and transportation), and delivery of capabilities corresponding to allied C4ISR capability targets will all contribute to the potential of NATO C4ISR.

As this report has highlighted, there are several areas where national defense spending and common funding are needed to ensure NATO C4ISR is fit for modern warfare and the threats and challenges identified in NATO's 2022 Strategic Concept. The following recommendations are an elaboration of key investment recommendations previously mentioned. Allies should:

- **Invest in NATO interoperability and integration.**
  - Accelerate development of C4ISR-related equipment and connectivity standards to ensure nations' disparate C4ISR systems and platforms (all types—C2, communications, computers, and ISR) can talk to each other and share real-time data and intelligence. This effort must address interoperability between national and proprietary cryptographic equipment and software.
  - Ensure adequate NATO staff support to nations in standards development.
  - Implement a NATO assessment mechanism to confirm the adoption of NATO standards by national and NATO C4ISR forces.
  - Review and act on the implications of NATO military assessments of C4ISR interoperability.
  - Leverage and support the potential of NATO's JISR interoperability trials (United Vision) to test, experiment, and validate C4ISR systems.
  - Adopt dual-use standards whenever possible to accelerate delivery of interoperable C4ISR capabilities or enablers.
- **Invest in NATO C4ISR force readiness and resilience.** Review manpower and resilience (cybersecurity, communications, and infrastructure) requirements of the NAEW&CF and NAGSF for MDO.
  - Invest in NATO C4ISR innovation and adaptation commensurate with NATO C4ISR's prominent role in shared awareness, decision-making, and action.
  - Include C4ISR challenges in the strategic guidance developed by nations for DIANA and the NATO Innovation Fund.
- **Invest in human capital development and management of leaders, operators, and intelligence professionals involved in or supporting NATO C4ISR.**
  - Invest in NATO C4ISR adaptation (and modernization) to meet the needs of the Alliance now and out to 2030 and beyond.
  - Ensure funding for DT requirements that will enable and enhance NATO C4ISR.
  - Plan for and invest in the modernization and future replacement of NAGSF platforms and systems.
  - Ensure funding of NATO commitments to AFSC and a fast-track approach for an advanced platform replacement for AWACS aircraft.

153 Patrick Goodenough, "Only 9 Out of 30 Allies Are Meeting NATO's Defense Spending Goal," *CNSNews*, June 30, 2022, https://www.cnsnews.com/article/international/patrick-goodenough/only-9-out-30-allies-are-meeting-natos-defense-spending.

CONCLUSION

NATO C4ISR capabilities have improved over the past decade but are not projected to meet future Alliance needs. Vulnerabilities and shortfalls persist, which are aggravated by a demanding security environment and an elevated level of NATO ambition agreed at the Madrid Summit. In particular, Russian aggression and other threats and challenges, including from terrorism, China, and climate change, raise requirements for speed and quality in NATO shared awareness, decision-making, and action. The latter are all enabled by NATO C4ISR.

The NATO 2022 Strategic Concept and recent policy decisions will set the context for future NATO C4ISR requirements. Future NATO defense planning and capability development of NATO C4ISR must respond to changing requirements and address critical issues. NATO has a unique window of opportunity over the next few years to leverage a newfound sense of cohesion and urgency among allies along with an agreed vision. Implementing recent NATO decisions, leveraging increases in defense investment, and exploiting proven or promising technologies present multiple opportunities to develop and deliver the C4ISR capabilities NATO forces need.

Five key efforts will maximize NATO's ability to maintain its comparative military advantage over the coming decade: improving data and intelligence sharing, transforming digitally, clarifying C4ISR architecture and requirements, modernizing or acquiring C4ISR capabilities and enablers, and continuing to invest in the ingredients of NATO's success for the past seven decades (i.e., interoperability, readiness, resilience, innovation, and adaptation).

GLOSSARY

A2CD2	Achieving and Accelerating Capability Development and Delivery
ACCS	Air Command and Control System
ACO	Allied Command Operations
ACT	Allied Command Transformation
AFSC	Alliance Future Surveillance and Control
AGS	Alliance Ground Surveillance
AI	artificial intelligence
AIRCOM	Air Command
AOR	Area of Responsibility
APSS	Alliance Persistent Space Surveillance
ASG	assistant secretary general
AWACS	airborne early warning and control system
C2	command and control
C3	consultation, command, and control
C4	command, control, communications, and computers
C4ISR	command and control, communications, computers, intelligence, surveillance, and reconnaissance
CMOSS	C4ISR/Electronic Warfare Modular Open Suite of Standards
CNAD	Conference of National Armaments Directors
COMINT	communications intelligence
C-UAS	counter-unmanned aircraft system
DCOS	Deputy Chief of Staff
DDA	Defense and Deterrence of the Euro-Atlantic Area
DEFP	Data Exploitation Framework Policy
DGIMS	Director General of the International Military Staff
DI	Defense Investment

DIANA	Defense Innovation Accelerator for the North Atlantic
DT	Digital Transformation
EDTs	emerging and disruptive technologies
ELINT	electronic intelligence
EM	electromagnetic
EMS	electromagnetic spectrum
EO	electrical-optical
EU	European Union
EW	electronic warfare
FMV	full-motion video
GBAD	ground-based air defense
GDP	gross domestic product
GPS	global positioning system
HQ	headquarters
HUMINT	human intelligence
I&W	indicators and warnings
IAMD	integrated air and missile defense
IEA	Information Environment Assessment
IMINT	imagery intelligence
IMS	International Military Staff
INF Treaty	Intermediate-Range Nuclear Forces Treaty
IoT	Internet of Things
IR	infrared
ISR	intelligence, surveillance, and reconnaissance
IT	information technology
JADC2	Joint All Domain Command and Control
JAPCC	Joint Airpower Competence Center

JFC	joint force command
JIS	Joint Intelligence and Security
JISD	Joint Intelligence and Security Division
JISR	joint intelligence surveillance and reconnaissance
MASINT	measurement and signature intelligence
MCR	Minimum Capability Requirements
MDO	multi-domain operations
ML	machine learning
NAC	North Atlantic Council
NAEW&CF	NATO Airborne Early Warning and Control Force
NAGSF	NATO Alliance Ground Surveillance Force
NATO	North Atlantic Treaty Organization and Reconnaissance
NCIA	NATO Communications and Information Agency
NCRS	NATO Crisis Response System
NDPP	NATO defense planning process
NHQC3S	NATO Headquarters C3 Staff
NIAG	NATO Industrial Advisory Group
NIE	NATO Intelligence Enterprise
NIF	NATO-Industry Forum
NIFC	NATO Intelligence Fusion Center
NMAs	NATO Military Authorities
NSPA	NATO Support and Procurement Agency
NWCC	NATO Warfighting Capstone Concept
OSINT	open-source intelligence
PDD	Public Diplomacy Division
PED	Processing, Exploitation, and Dissemination
R&D	research and development

SACEUR	Supreme Allied Commander Europe
SACT	Supreme Allied Commander Transformation
SASP	SACEUR's Area of Responsibility-Wide Strategic Plan
SBAMD	Surface-Based Air and Missile Defense
SHAPE	Supreme Headquarters Allied Powers Europe
SIGINT	signals intelligence
SMEs	small and medium-sized enterprises
STO	Science & Technology Organization
TCPED	Tasking, Collection, Processing, Exploitation, and Dissemination
TDL	Tactical Data Link
UAS	unmanned aircraft system

ABOUT THE AUTHOR

Gordon B. “Skip” Davis Jr. is currently a Senior Fellow at the Center for European Policy Analysis. He recently served as NATO’s Deputy Assistant Secretary General for Defense Investment. Prior to NATO, Skip served 37 years in the U.S. Army retiring as a Major General. Skip’s last military positions were as Director of Operations, U.S. European Command, Commander of Combined Security Transition Command – Afghanistan, and Director of Operations and Intelligence for Allied Command Operations. Skip’s professional life included operational and institutional assignments interspersed with study and practice of international affairs and defense issues, primarily in Europe. Skip participated in operations with U.S., NATO, and UN forces in Europe, Africa, Middle East, and Central Asia. Skip brings practical experience and conceptual understanding of contemporary and emerging defense issues as well as executive-level experience in operations, intelligence, leader development, capability development, and policy development. Skip holds an undergraduate degree in nuclear physics and graduate degrees in international business, defense and military history, and strategic studies.

Mr. Davis and his wife Rita have two daughters, Stefania and Victoria, both of whom completed their undergraduate degrees in Italy. Stefania is a promotable Captain in the U.S. Military Intelligence Corps serving in Wiesbaden, Germany, and Victoria is a linguist and performing artist working in Washington, D.C.

Atlantic Council

Board of Directors

CHAIRMAN
*John F.W. Rogers

EXECUTIVE CHAIRMAN EMERITUS
*James L. Jones

PRESIDENT AND CEO
*Frederick Kempe

EXECUTIVE VICE CHAIRS
*Adrienne Arsht
*Stephen J. Hadley

VICE CHAIRS
*Robert J. Abernethy
*C. Boyden Gray
*Alexander V. Mirtchev

TREASURER
*George Lund

DIRECTORS
Todd Achilles
Timothy D. Adams
*Michael Andersson
David D. Aufhauser
Barbara Barrett
Colleen Bell
Stephen Biegun
Linden P. Blue
Adam Boehler
John Bonsell
Philip M. Breedlove
Richard R. Burt
*Teresa Carlson
*James E. Cartwright
John E. Chapoton
Ahmed Charai
Melanie Chen
Michael Chertoff
*George Chopivsky
Wesley K. Clark
*Helima Croft
*Ankit N. Desai
Dario Deste
Lawrence Di Rita
*Paula J. Dobriansky
Joseph F. Dunford, Jr.
Richard Edelman
Thomas J. Egan, Jr.
Stuart E. Eizenstat
Mark T. Esper
*Michael Fisch
Alan H. Fleischmann
Jendayi E. Frazer
Meg Gentle
Thomas H. Glocer
John B. Goodman
*Sherri W. Goodman
Jarosław Grzesiak
Murathan Günal
Michael V. Hayden
Tim Holt
*Karl V. Hopkins
Kay Bailey Hutchison
Ian Ihnatowycz
Mark Isakowitz
Wolfgang F. Ischinger
Deborah Lee James
*Joia M. Johnson
*Safi Kalo
Andre Kelleners
Brian L. Kelly
Henry A. Kissinger
John E. Klein
*C. Jeffrey Knittel
Joseph Konzelmann
Franklin D. Kramer
Laura Lane
Almar Latour
Yann Le Pallec
Jan M. Lodal
Douglas Lute
Jane Holl Lute
William J. Lynn
Mark Machin
Marco Margheri
Michael Margolis
Chris Marlin
William Marron
Christian Marrone
Gerardo Mato
Erin McGrain
John M. McHugh
*Judith A. Miller
Dariusz Mioduski
Michael J. Morell
*Richard Morningstar
Georgette Mosbacher
Majida Mourad
Virginia A. Mulberger
Mary Claire Murphy
Edward J. Newberry
Franco Nuschese
Joseph S. Nye
Ahmet M. Ören
Sally A. Painter
Ana I. Palacio
*Kostas Pantazopoulos
Alan Pellegrini
David H. Petraeus
*Lisa Pollina
Daniel B. Poneman
*Dina H. Powell McCormick
Michael Punke
Ashraf Qazi
Thomas J. Ridge
Gary Rieschel
Michael J. Rogers
Charles O. Rossotti
Harry Sachinis
C. Michael Scaparrotti
Ivan A. Schlager
Rajiv Shah
Gregg Sherrill
Jeff Shockey
Ali Jehangir Siddiqui
Kris Singh
Walter Slocombe
Christopher Smith
Clifford M. Sobel
James G. Stavridis
Michael S. Steele
Richard J.A. Steele
Mary Streett
*Gil Tenzer
*Frances F. Townsend
Clyde C. Tuggle
Melanne Verveer
Charles F. Wald
Michael F. Walsh
Ronald Weiser
*Al Williams
Maciej Witucki
Neal S. Wolin
*Jenny Wood
Guang Yang
Mary C. Yates
Dov S. Zakheim

HONORARY DIRECTORS
James A. Baker, III
Robert M. Gates
James N. Mattis
Michael G. Mullen
Leon E. Panetta
William J. Perry
Condoleezza Rice
Horst Teltschik
William H. Webster

**Executive Committee Members*

List as of March 6, 2023

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.

Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org