



NATO Command and Control Resilience in Contested Environments

X11

*By Mr Owen J. Daniels and
Ms Clementine G. Starling*

*Institute for Defense Analyses/Scowcroft Center for
Strategy and Security, Atlantic Council*

As competitors aim to disrupt communication and coordination among NATO forces, the Alliance's ability to maintain Command and Control (C2) will be paramount. NATO must adapt to improve its C2 resiliency and consider new concepts for operating in contested environments, especially as Allies explore technological and systematic changes to their C2 structures. The United States is adapting its C2 structure with concepts like Joint All Domain Command and Control (JADC2) and NATO Allies should weigh similar approaches to bolster combat effectiveness, ensure integration, and maintain interoperability in degraded C2 environments. This article presents ongoing and future C2 challenges for NATO and possible approaches for improving C2 resiliency.

NATO's C2 Challenge in Contested Environments

Russia poses the most likely contested environment dilemma for NATO. Russian Anti-Access/Area Denial (A2/AD) tactics could limit NATO's ability to establish strategic advantage at its doorstep even before

a conflict, disrupting NATO efforts when 'fait accompli' scenarios erupt.^{1,2} A2/AD prevents opponents from accessing key areas and denies manoeuvre, allowing adversaries temporal advantages to achieve effects before the warfighting space can be contested. Anti-access could prevent NATO from projecting power into the battlespace, enabling adversaries to favourably change facts on the ground. The S-400, Bastion anti-ship system, and Iskander ballistic missile comprise the core of Russia's A2/AD suite and work in concert as deterrents against potential NATO responses to aggression.³ Russia demonstrates its denial capabilities in the Arctic, Baltic, and Black Sea regions; no-go 'bubbles', like the Kaliningrad exclave, aim to deter NATO action by signalling impregnability.⁴

NATO's C2 nodes and infrastructure in kinetic and non-kinetic domains, critical to any contingency fight, will likely be among the first targets in a contested environment. Operational C2 impacts battle management and forward force projection – disrupting it holds appeal for adversaries less capable than NATO. C2 denial could complicate NATO's vision for supplying, sustaining, and reinforcing forward forces, like enhanced Forward Presence battlegroups in the Baltics, and disrupt NATO's overall force projection ability and collective response. In manoeuvre warfare, A2/AD disrupts information flows and command between sensors and shooters. With inadequate preparation, tactical forces could struggle to contribute to combined effects, hampering the strength of the force. Further, NATO's air power is vulnerable to electronic warfare platforms that seek to disrupt its forces' communications, coordination, and target identification capabilities.⁵

The Alliance struggles with interoperability and C2 at the best of times; differing command styles, technology, capabilities, and terminology complicate communication among nations and within a blended chain of command. Standardization and basic military equipment compatibility challenges hinder NATO in peacetime; adversaries exploiting NATO's C2 vulnerabilities will only exacerbate these problems.

During the past year, Allies have started to adapt their operational concepts to address these challenges. The UK's Joint Concept Note (JCN) 1/20 for Multi-Domain Integration (MDI) focuses on 'integrating for advantage' across domains and levels of warfare, along with allies and partners.^{6,7} Similarly, the US JADC2 concept mixes new technologies and capabilities with adapted tactics, techniques, and procedures.⁸ By examining Allies' newly proposed doctrinal solutions to the C2 problem, NATO can anticipate its own implementation challenges and identify key areas for future adaptation.

Preparing for the Future of C2

Effective C2 among Allies will require commanders and operators to operationally, if not necessarily technically, understand the cross-cutting nature of Multi-Domain Operations (MDO). NATO is already acting on this: its MDO C2 Demonstrator platform⁹ acknowledges the existence of kinetic and non-kinetic threats to the Alliance and the impact of cross-domain effects.¹⁰ NATO's Joint Warfare Centre (JWC) provides collective joint warfare training, and the North Atlantic Council (NAC) directed a Joint Effects function under the NATO Command Structure Adaptation (NCSA). Additionally, the Fires and Effects Synchronization Board addresses MDO challenges, including coordinating lethal and non-lethal effects through the NATO J-3.¹¹ Previously commissioned NATO studies, including SAS-085 and SAS-110, have endeavoured to nuance the Alliance's thinking about C2 relationships in complex environments, recognizing the importance of C2 agility¹² to account for diverse mission sets, command styles, and changing conditions within particular missions.¹³ While these developments are promising, Allies are not advancing interoperable C2 systems rapidly enough, and NATO could do more to advance coordinating authorities for implementing MDO concepts.

Protecting shared understanding of the situational picture will be critical to enabling effective C2 of MDO; NATO should address critical cyber vulnerabilities in its Joint Intelligence, Surveillance and Reconnaissance (JISR) architecture. JISR provides timely information support including collecting, processing, and disseminating information across multiple domains from national assets.¹⁴ Operationalizing an MDO concept will require NATO's JISR Task Force, Intelligence Fusion Centre, Joint Force Commands, and component commands to remain closely integrated to ensure that ISR is rapidly disseminated to strategic and tactical leaders.

Experimentation and subsequent exercises can begin to address changing C2 structures and improve readiness for future challenges. So long as C2 threats remain imminent, a robust experimentation program will be necessary to determine new approaches and uncover gaps, costs, and risks. NATO must also prioritize C2 experimentation across environments and scenarios.¹⁵ When experimentation leads to new solutions and courses of action, continuously exercising NATO's strategic, operational, and tactical C2 will be necessary. NATO's Trident Juncture 2018 exercise and the US-led Defender Europe 20 enabled allies and partners to rehearse integrating C2 by rotating command responsibilities in different theatres with varying participants. However, as allies update their C2 structures and create command elements to absorb, NATO must prevent C2 becoming its Achilles heel. Training and exercises must incorporate complex denial scenarios that stress test C2 and specifically simulate operations amid degraded C2.

NATO has discussed developing an enterprise-wide architecture for its future C2 capabilities.¹⁶ It should capitalize on technological innovations in Allies' ISR, Space, Cyberspace, and electromagnetic capabilities to bolster resilience. While some Allies are likely to take the lead on technological 'big bets,' NATO should look for ways to integrate national

technological advancements for the wider Alliance’s benefit. For example, the Alliance could experiment with technologies that gracefully degrade, or retain some function after critical processes are disrupted, or alternatively test new approaches that are more decision- and less data-centric.¹⁷ Through NATO’s Defence Planning Process, the Alliance should harmonize changing national plans and capability development, and could add graceful degradation-specific capability goals to its Minimum Capability Requirements.

NATO must also look beyond purely technical fixes to its strategy, operations, techniques, and procedures. Reliance on robust, high-bandwidth communications has been a hallmark of NATO operations, but these C2 channels will likely be disrupted in contested environments, requiring an appropriate mix of robust C2 capabilities and effective mission orders and tactics suitable for communications-denied environments. At a high level, NATO should consider new strategic or multi-domain operational concepts that address the challenges inherent in contested operating environments. From a US perspective, MDO nest under the concept of joint operations.¹⁸ NATO joint staffs and the JWC could explore creating a NATO MDO concept to align joint warfare approaches across the Alliance.

New concepts may require new thinking about command authorities and authorizations. Determining the degree of autonomy that subordinates should possess to adapt to disrupted C2 and achieve the commander’s intent in light of new member nation C2 plans is worth examining in the NATO context. The importance of C2 that is attuned to the environment and capable of shifting mid-operation should lead NATO leaders to consider decentralized command structures that empower staff to respond ‘in the moment’ more effectively.¹⁹ For example, the US Air Force phrase ‘centralized control, decentralized execution’²⁰ highlights the principle of decentralizing command to soldiers,

enabling them to exercise decisions if cut off from the chain of command. Lower-level decision-making could improve speed, C2 agility, and effectiveness while more easily cutting across domains and joint force structures. Thinking about NATO C2 from the bottom-up may generate insights into best practices for survivability and linking distributed tactical nodes.²¹ This approach must be inculcated into the professional culture to succeed and will require experimentation to determine relevant and potentially new practices.²² For NATO forces to operate based on commander's intent amid degraded C2 conditions, doctrine, education, training, and exercises must adapt accordingly. US-led training with Allied forces could demonstrate how diffused C2 works in practice and could help Allies develop their own concepts.

Recommendations

As NATO grapples with greater C2 challenges, it can take several steps to improve its C2 resiliency.

First, the Alliance should consider adopting a NATO-wide MDO concept. A concept could help initially frame how to assess capabilities and determine roles in an interoperable C2 architecture. Wargaming and experimentation will be important for testing and validating the new concept, and red teaming and tabletop exercises can expose the seams between Allies and can highlight vulnerable nodes. This testing may also expose bureaucratic, technical, and cultural obstacles.

Second, when a concept is in place, NATO should conduct an Alliance-wide assessment to determine which Allies and partners are developing critical capabilities to support operators at C2 nodes. Allies must prioritize developing interoperable C2 systems with compatible equipment to mitigate gaps.

Third, NATO should establish common goals and criteria to measure progress towards interoperability and preparedness for C2 resilience. A 2013 US Joint Wargame assessing C2 in the context of the Air-Sea Battle concept identified unity of effort, flexibility, simplicity, resiliency, operational integration, and cross-domain synergy as performance indicators.²³ Future assessments should also include how C2 progresses during an exercise as it would during operations.²⁴ By adopting such goals and criteria, the Alliance can create benchmarks for measuring its progress and determining priorities based on need and ability.

Fourth, NATO will need to exercise for contested environments at scale to prepare for decentralized C2, test different force mixtures, and determine how best to exploit human-machine teaming and unmanned system advantages. It should exercise varied scenarios of C2 degradation and operations in denied environments. NATO will also need to reckon with the hard realities that decentralized C2 creates for coordinating wide-ranging MDO effects with limited communications. The US-led, multinational exercise Bold Quest is an example NATO could build upon in the future.

Preparing for the likelihood of degraded C2 is critical if NATO is to better prepare for future crises. Adversary efforts to disrupt C2 should not pitch the entire enterprise into the dark. Rather, resilient systems and agile, decentralized processes should enable Allies to take C2 attacks in stride. NATO must improve C2 resilience, interoperability, and compatibility of Allied C2 systems by investing in technology with graceful degradation capacity; adapting exercises and training to include denied environment scenarios; and exploring decentralized C2 doctrine. As technology has evolved, adversaries' opportunities for and ability to thwart NATO C2 has increased. NATO must start to strengthen its resilience for tomorrow.

Mr Owen Daniels is a research associate in the Joint Advanced Warfighting Division at the Institute for Defense Analyses in Alexandria, Virginia. He previously worked in the Scowcroft Center for Strategy and Security at the Atlantic Council and at Aviation Week magazine, and leads Young Professionals in Foreign Policy's Fellowship Program.

Ms Clementine G. Starling is a resident fellow and the deputy director of Forward Defense at the Atlantic Council. Starling's research focuses on great power competition with China and Russia, deterrence, US defense policy, and transatlantic security. Prior to joining the Atlantic Council, she worked in the UK House of Commons.

Endnotes

1. Kofman, Michael, 'It's Time to Talk about A2/AD: Rethinking the Russian Military Challenge,' War on the Rocks, 5 Sep. 2019 [Online]. Available: <https://warontherocks.com/2019/09/its-time-to-talk-about-a2-ad-rethinking-the-russian-military-challenge/>.
2. Schmidt, Andreas, 'Countering Anti-Access/Area Denial: Future Capability Requirements in NATO,' JAPCC Journal 23 [Online]. Available: <https://www.japcc.org/countering-anti-access-area-denial-future-capability-requirements-nato/>.
3. Williams, Ian, 'The Russia-NATO A2AD Environment,' CSIS, 3 Jan. 2017 [Online]. Available: <https://missilethreat.csis.org/russia-nato-a2ad-environment/>.
4. Dalsjo, R., Jonsson, M., Berglund, C., 'Don't Believe the Russian Hype,' Foreign Policy, 7 Mar. 2019 [Online]. Available: <https://foreignpolicy.com/2019/03/07/dont-believe-the-russian-hype-a2-ad-missiles-sweden-kaliningrad-baltic-states-annexation-nato/>.

5. Smith, Patrick, 'Russian Electronic Warfare,' American Security Project, Apr. 2020, pp. 3 [Online]. Available: <https://www.americansecurityproject.org/wp-content/uploads/2020/04/Ref-0236-Russian-Electronic-Warfare.pdf>.
6. UK Ministry of Defence, 'Multi-Domain Integration (JCN 1/20),' 2 Dec. 2020 [Online]. Available: <https://www.gov.uk/government/publications/multi-domain-integration-jcn-120#:~:text=This%20integration%20must%20be%20across,domains%20and%20levels%20of%20warfare.>
7. UK Ministry of Defence, 'Integrated Operating Concept 2025,' 30 Sep. 2020 [Online]. Available: <https://www.gov.uk/government/publications/the-integrated-operating-concept-2025>.
8. Hoehn, John, 'Joint All-Domain Command and Control (JADC2),' Congressional Research Service [Online]. Available: <https://fas.org/sgp/crs/natsec/IF11493.pdf>.
9. NATO C2COE, 'The NATO C2COE MDO C2 Demonstrator platform,' 11 Jun. 2020. [Online]. Available: <https://c2coe.org/download/the-nato-c2coe-mdo-c2-demonstrator-platform/>.
10. Freedburg, Jr., Sydney, 'Target, Kaliningrad: Air Force Puts Putin On Notice,' Breaking Defense, 17 Sep. 2019 [Online]. Available: <https://breakingdefense.com/2019/09/target-kaliningrad-eucom-puts-putin-on-notice/>.
11. Jones, M. and Diaz de Leon, J., 'Multi-domain Operations,' The Three Swords Magazine, 36/2020, pp. 40–41 [Online]. Available: https://jwc.nato.int/application/files/5616/0523/5418/issue36_08lr.pdf.
12. C2 Agility is the capability of C2 to successfully effect, cope with, and/or exploit changes in circumstances. C2 Agility enables entities to effectively and efficiently employ resources in a timely manner. NATO Task Group SAS-085 Final Report on C2 Agility, 2014 [Online]. Available: http://www.dodccrp.org/sas-085/sas-085_report_final.pdf.
13. NATO Task Group SAS-085 Final Report on C2 Agility, 2014 [Online]. Available: http://www.dodccrp.org/sas-085/sas-085_report_final.pdf.
14. Ferguson III, M., Harper, C., Hooker, R., 'Over The Horizon,' Atlantic Council, 14 Nov. 2019, pp. 3 [Online]. Available: <https://www.atlanticcouncil.org/in-depth-research-reports/report/over-the-horizon-nato-joint-intelligence-surveillance-and-reconnaissance-in-the-baltic-sea-region/>.
15. Ibid. 12.
16. Sirota, Sara, 'NATO to develop new air command and control capability architecture,' Inside Defense, 14 Jan. 2020 [Online]. Available: <https://insidedefense.com/insider/nato-develop-new-air-command-and-control-capability-architecture>.
17. Czarnecki, J., and Chamberlain, T., 'Graceful Degradation: A C2 Virtue for Our Times,' 18th ICCRTS, California: Naval War College, Aug. 2018.
18. Jones, Leon, 'Multi-domain Operations,' The Three Swords Magazine, 36/2020, pp. 38–41 [Online]. Available: https://jwc.nato.int/application/files/5616/0523/5418/issue36_08lr.pdf.
19. Tillman, M.E. and Conley, K.M., 'Designing and Assessing Command and Control to Deal with Complex and Ill-Structured Operational Environments.' In Operations Assessment in Complex Environments: Theory and Practice, edited by Adam Shilling. NATO STO, 2019.
20. Hinote, Clint, 'Centralized Control and Decentralized Friction,' Air University Air Force Research Institute, Mar. 2009 [Online]. Available: https://media.defense.gov/2017/Jun/19/2001764937/-1/-1/0/AP_0006_HINOTE_CENTRALIZED_CONTROL_DECENTRALIZED_EXECUTION.PDF.
21. Birch, P., Reeves, R., and Dewees, B., 'Building the Command and Control of the Future from the Bottom Up,' War on the Rocks, 16 Jan. 2020 [Online]. Available: <https://warontherocks.com/2020/01/building-the-command-and-control-of-the-future-from-the-bottom-up/>.
22. US Marine Corps, 'MCDP-1 Warfighting,' Jun. 1997 [Online]. Available: <https://www.marines.mil/Portals/1/Publications/MCDP%201%20Warfighting.pdf>.
23. US Department of Defense, 'Air Sea Battle,' May 2013 [Online]. Available: <https://archive.defense.gov/pubs/ASB-ConceptImplementation-Summary-May-2013.pdf>.
24. Ibid. 18.