FINABEL
THE EUROPEAN LAND FORCE
COMMANDERS ORGANISATION

OCTOBER 2025

NATO's Codification Gap:
Why Joint ISR Still Falls Short

Kevin Whitehead
Defence & Security Research Department

RESEARCH REPORT

FINABEL
THE EUROPEAN LAND FORCE
COMMANDERS ORGANISATION

Defence & Security Research Department

Written by: **Kevin Whitehead**
Supervised by: **Elise Alsteens**
Edited by: **Theodora Posta**

FINABEL's Research Reports are concise, research-driven publications designed to keep Europe's defence community informed about the latest strategic, military, and geopolitical developments. Released three times per week, these short-form papers offer timely analysis on emerging trends affecting European land forces. Each Research Report is produced by the researchers of FINABEL's Permanent Secretariat, in the goal of supporting decision-making across the European defence landscape.

RESEARCH REPORT

Introduction

NATO's Joint Intelligence, Surveillance and Reconnaissance (JISR) system works as the Alliance's nervous system, by connecting data sensors to military leaders across all domains (NATO, 2025; Gilli, 2025). While Intelligence, Surveillance and Reconnaissance (ISR) refers to the collection and processing of information, JISR emphasizes the integration and sharing of intelligence across NATO (NATO, 2025). Over the past decades, NATO has made great progress in strengthening capabilities – including new platforms, networks and doctrines – yet its intelligence sharing system remains insufficient (Davis, 2023). This gap between goals and real capabilities reveals serious risks. In a future crisis, NATO's credibility could be undermined if intelligence can only be integrated once the crisis occurs. It is not feasible for the Alliance to create new ISR sharing tactics and procedures in the middle of an operation. Without a fully codified and integrated ISR posture, NATO may struggle to provide timely, quality intelligence in the moments when it needs it the most.

This article poses the question why NATO has failed to fully codify its JISR efforts despite significant progress, and what reforms are needed to close what is labelled the codification gap. In this context, the 'codification gap' refers to NATO's tendency to adapt ISR practices during crises, but to fall short of translating these adaptions into binding standards and enforceable mechanisms. Analysts note that NATO lacks enforcement authority to ensure compliance with alliance-wide standards (Riedenstein, Echikson, & Landrum, 2025), while its ISR-sharing posture remains hindered by insufficient codification of standards (Davis, 2023). It argues that the existing technical, political, and institutional frictions have hurt the Alliance's ability to institutionalize joint ISR. The article begins by looking at the evolution of NATO's ISR: from the shortcomings exposed in Libya and Afghanistan, to the improvements seen during the war in Ukraine. It then examines how interoperability challenges, security caveats, and a reliance on voluntary national contributions continue to restrict JISR codification. Finally, the article proposes possible actions to move NATO's ISR from a voluntary system towards a truly unified capability for the Alliance.

1. From Libya to Ukraine: Lessons on ISR Gaps

1.1 *Libya 2011 (Operation Unified Protector)*

NATO's 2011 intervention in Libya exposed the Alliance's dependence on ad hoc intelligence support. The United States flew roughly 80% of ISR and air-refuelling missions (Greenleaf, 2013). NATO also relied on U.S. communications networks and trained personnel to process and integrate ISR data (Martin, 2014). Allied commands were able to "cross-cue" sensors and striking targets, but the process took months before becoming fully operational (Martin, 2014). Additionally, shortcomings in Libya were linked to a lack of "trained Joint ISR personnel, outdated NATO Joint ISR doctrine and procedures, and a lack of connectivity" (Murray, 2016, para. 3). In short, NATO entered the Libya conflict without common ISR standards or a preexisting framework for sharing real-time intelligence. Post-operation analyses of NATO's 2011 Libya campaign identified ISR as a critical shortfall, pointing to a scarcity of available assets, inadequate sharing mechanisms, and heavy reliance on U.S. capabilities (NATO, 2012; Gotkowska, 2013). As former

Secretary General Anders Fogh Rasmussen said, “Libya revealed shortfalls in... intelligence, surveillance and reconnaissance assets, and experts trained to interpret the data they provided” (Haider, Menzel, & Perkins, 2015, p. 13). While work has begun to close these gaps, the lessons was clear that NATO needed a more integrated approach to ISR.

The Libya case ultimately shows what this paper calls the “codification gap”. NATO improvised workarounds under pressure, but it lacked the institutional standards and mechanisms that would have allowed joint ISR to function efficiently from the start. The Alliance’s reliance on U.S. assets, month-long struggle to align procedures, and the lack of trained personnel highlights that NATO did not suffer from a lack of awareness, but rather from a lack of codified practices. Libya revealed that without common frameworks, ISR effectiveness will continue to hinge on U.S. support and on ad hoc learning curves. This over-reliance on improvisation is the risk NATO faces in future crises. Therefore, the lessons of Libya point out the importance of moving towards codified standards that guarantee interoperable ISR as a capability.

1.2 *Afghanistan (International Security Assistance Force, ISAF)*

In contrast to Libya’s ad hoc solutions, Afghanistan demonstrated that NATO could experiment with federated networks, showing both their limits and their potential. At the start of the ISAF mission, coalition ISR sharing remained hindered by national ‘need-to-know’ security rules and incompatible national systems, which fragmented intelligence and restrained situational awareness (Serena et al., 2014). Contributors often relied on separate networks rather than a common platform, leaving intelligence sharing mainly halted across NATO. To overcome these barriers, NATO set up the Afghan Mission Network (AMN) in 2010 as a common classified network, and the AMN allowed 48 contributing NATO and partner nations to share intelligence within a single system (Serena et al., 2014; Jacobs, 2014). This required a cultural shift, driven by General Stanley McChrystal’s emphasis on replacing the old ‘need-to-know’ mindset with a ‘need-to-share’ culture (Serena et al., 2014).

The result was a federated network that dramatically improved coalition ISR coordination. As one U.S. officer observed, “NATO overcame many difficulties to stand up the Afghan Mission Network so coalition members could share intelligence data... [It] helped to bridge the intelligence gap created by numerous national intelligence networks” (Wittstruck, 2015, p. 29). For the first time, a formal system allowed a troop force from one NATO country to view sensor feeds or reports from another nation’s assets. The AMN’s success showed that with political will and agreed standards, and a formal system, fragmented allies could effectively use a unified ISR network. This revealed NATO’s tendency to only codify lessons after-the-fact, rather than build frameworks during operations. In 2012, NATO launched the Federated Mission Networking (FMN) initiative to institutionalize AMN’s lessons (Serena et al, 2014; NATO, 2012). This shows a pattern where NATO adapts effectively during missions, but often only later go through the lengthy process of codifying these initiatives alliance-wide.

The Afghanistan case shows both progress and limitations. AMN proved that NATO could overcome fragmented systems and create an efficient federated ISR network. Yet, its mission-specific status illustrates

the Alliance's reliance on operational urgency to push progress ahead. Instead of immediately institutionalizing AMN, NATO required a separate political decision to launch FMN years later. This delay further shows the codification gaps: whereas ISR advances under pressure, the process of turning the results into NATO-wide standards remains slow and reactive. In sum, Afghanistan demonstrated that, while federated solutions are possible, they remain tied to temporary missions, unless they are codified into Alliance agreements.

1.3 *Ukraine*

Russia's war against Ukraine has shown both NATO's progress on ISR integration, as well as its continued struggle to codify this progress. Unlike in Libya and Afghanistan, where ISR challenges were only addressed after operational failures, NATO undertook reforms proactively following Russia's 2014 annexation of Crimea. Allies established new coordination mechanisms, such as the Joint Intelligence and Security Division (2016), and invested in capabilities like the Alliance Ground Surveillance (AGS) drones, which became operational in 2020 (Freytag von Loringhoven, 2017; Horrell, 2022). These measures showed that NATO could institutionalize lessons outside of the context of a crisis. However, the 2022 invasion revealed the limits of these reforms. While AGS flights over the Black Sea and NATO's AWACS patrols provided improved situational awareness (NATO, 2025; Horrell, 2022), ISR effectiveness still relied on a small number of shared assets rather than a fully integrated system. In practice, reforms narrowed earlier gaps, but were not codified into enforceable obligations, leaving NATO dependent on voluntary national contributions. A distinctive feature of the Ukraine case was the use of 'public intelligence'. In the lead up to the invasion, the United States and the United Kingdom publicly declassified intelligence (eight disclosures) about Russian troop movements, to expose Russia's plans and build allied cohesion (Brattvoll, 2024; Marleku, 2025). This was effective in countering disinformation, yet it remained an ad hoc political choice outside NATO doctrine. Ultimately, Ukraine shows both progress and persistence of the codification gap. Compared to Libya and Afghanistan, Ukraine demonstrates that proactive reforms are possible, but without binding standards and codification, these advances risk remaining ad hoc.

2. Persistent Frictions

Despite progress in this sphere, NATO still faces significant challenges that hinder the Implementation of NATO technical standards is uneven, however, and largely reliant on national implementation rather than a single, enforced NATO-wide verification system (Huismans et al., 2025). The result is that ISR systems of one ally may not be able to share data efficiently to the system of another if standards are not met. Indeed, uncoordinated national upgrade programs risk "exacerbating interoperability gaps" and fragmenting NATO's ISR architecture (Gilli, 2025, p. 1). European Allies' underinvestment in past decades has left many depending on old platforms, which reinforces this issue (Gilli, 2025). Exercises like Unified Vision and CWIX have helped solve many technical issues (NATO, 2018), yet NATO still lacks consistent standards, verifiable certification, and agreed metrics for interoperability (U.S. Army College, 2025). Without these, NATO risks having to rebuild JISR in each crisis on an ad hoc basis, rather than maintaining a fully unified system.

On the other hand, NATO's progress towards a unified ISR system is additionally being held back by political barriers. Allies remain reluctant to share intelligence fully and one persistent obstacle is over-classification. The Atlantic Council argues that excessive use of the NOFORN caveats – U.S. classification marking that prohibits sharing information with non-U.S. personnel – and restrictive classification rules undermines allied intelligence sharing (Corbett & Danoy, 2022). The U.S. Defense Innovation Board additionally observes that Washington's tendency to default to NOFORN and restrictive disclosure policies generate friction with allies and hinder operational collaboration (Defense Innovation Board, 2024). This directly contrasts the Alliance's doctrine of 'responsibility to share', outlined in NATO's JISR framework. Diverging political priorities further complicate integration. NATO's eastern members view Russia as the primary threat, while southern states prioritize terrorism and migration (Davidson, 2025). This affects the attitude of political choices, and shapes investment choices and willingness to share. Additionally, burden-sharing debates also exist where European underinvestment has left critical ISR modernization slow. IISS notes that "low numbers of European intelligence, surveillance and reconnaissance (ISR) aircraft and limited geospatial ISR collection remain a major concern" (IISS, 2025).

Lastly, institutional and policy shortcomings remain a major source of friction in NATO's intelligence sharing as well. Despite reforms such as JISD, the Alliance still lacks enforceable standards and mechanisms to ensure consistent national practices. Most ISR sharing arrangements remain voluntary. Unlike NATO's defence spending pledge, which sets a concrete 2 percent of GDP and relies on pressure to encourage compliance, there is no equivalent metric for intelligence contributions. Allies are not formally required to provide specific products or connect their databases to NATO networks. This leaves NATO in a state where participation is encouraged, but not enforced. This creates a codification gap where initiatives may be approved, such as new data-sharing systems, without any guarantee that nations will contribute to them. As the Centre for European Reform notes, NATO has no legal enforcement tools in this area and must rely on consensus and peer pressure (Besch, 2018). The absence of formal integration into force planning adds to this issue. There is no 'intelligence sharing readiness' metric or feedback loops to identify the lessons learned. While NATO conducts after-action reports for operations, intelligence is often left out, with reforms happening ad hoc or through the efforts of a few leading states. Governance is further complicated by multiple stakes. As the Alliance relies on voluntary contribution, the result is that intelligence sharing remains inconsistent. Closing this gap would likely require formal agreements or incentives that make sharing the default option. However, for these to be truly codified, it would require for them to be backed by oversight to identify and address problems. In the absence of such a measure, NATO will continue to depend on the right political climate to align for effective ISR cooperation. This poses a vulnerability in any future crisis that demands guaranteed cohesion.

3. Policy Implications

To transform NATO's JISR from a voluntary system into a codified capability, the Alliance will need a reformative policy initiative. The following reforms address the technical, political, and institutional frictions identified above.

Firstly, Nato could integrate specific ISR targets into its defence planning process, similar to the 2 percent GDP defence spending pledge. This means defining concrete capability goals for ISR that each Ally commits to meet. A first step is providing clear minimum standards for Allied Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR), which needs improvement (Davis Jr., 2023). By establishing agreed upon standards, NATO could hold nations accountable for building pieces of a joint ISR system. In essence, JISR should move from a voluntary contribution status to a formal requirement in NATO's force structure. Codifying these expectations would incentivize investments and help even out disparities between U.S. and European capabilities; this has been seen since the initiation of the 2 percent GDP spending pledge, where from 2014-2023, NATO European Allies and Canada have invested $350 billion (Grand, 2023). NATO must improve C4ISR with common standards across the force, by writing JISR into the force plan and reviewing it regularly. This would make it a mandated topic of discussion.

Secondly, the Alliance could institute metrics to measure how prepared and willing members are to share intelligence. Just as NATO rates the readiness of combat units into readiness tiers (eg. 0-10 days, 10-30 days, 30-80 days) (NATO, n.d.), the Alliance could develop an intelligence-readiness metric to measure how quickly Allies produce and share satellite imagery or how many trained intelligence personnel they have available. For example, by measuring how quickly a nation can produce satellite imagery or other data to NATO in a crisis, or by how many intelligence staff it has trained. These metrics would aim to quantify the intangible contributions of information, and thus reveal gaps and provide accountability. If certain Allies fail to share their contributions during exercises, NATO would be able to pinpoint the issue and address it. The goal would be to create a culture of expected sharing as part of NATO's operational readiness. Over time, publishing these metrics would pressure those at the bottom to contribute more.

Thirdly, NATO could make Joint ISR integration drills a part of training exercises. The Unified Vision exercises have already started to connect "NATO or national systems" in realistic scenarios. NATO should expand Unified Vision into a regular annual event to test Allies' ISR capabilities and interoperability. During the Unified Vision 2023 exercise, for example, 18 Allies tested their ability to collect, process, and share intelligence using 25 maritime, land, air and space assets (NATO, 2023). This would allow multinational ISR assets and analysts to practice as a unified force in real-like scenarios. The evaluations of these exercises would enforce technical standards and build trust in sharing. By making combined ISR exercises as regular as combat exercise, NATO will ensure interoperability issues are solved proactively rather thanduring a current crisis moment.

Lastly, NATO needs a political agreement to lower over-classification. A practical step would be implementing a tiered NATO-wide intelligence release policy. Instead of choosing between sharing or NOFORN, information could be labelled for release to all Allies by default, with exceptions for highly sensitive information. For example, the United States and others could agree to list intelligence as approved for NATO as the norm, rather than defaulting to national-only restrictive classification. The Atlantic

Council, for example, has advised that the NOFORN caveats be used only on rare occasions as an expectation (Corbett & Danoy, 2022). In sum, NATO should strive towards a secure information system that allows information to reach all Allies in real time, once that information is cleared. The goal is to change the incentive so that countries don't prefer to hold information, but rather default on sharing to all Allies. By establishing a sharing system that promotes connectivity, the Alliance can fulfill their 'responsibility-to-share' strategy.

Conclusion

From Libya's ad hoc solutions to Afghanistan's federated fixes and Ukraine's mixed successes, it is clear that NATO innovates during crises, but struggles to codify in peacetime. This leaves the Alliance with a fragile posture that depends on leader decisions, over-classification, and U.S. capabilities when problems appear. Technical progress has been made, yet uneven adoption of standards, old digital systems, and fragmented innovation strategies still hurts data sharing. Political friction is seemingly the largest challenge. Issues like national caveats, NOFORN defaults, and divergent threat priorities affect the Alliance's responsibility to share. Institutionally, NATO lacks enforceable power, common metrics, and certification that would make JISR solidified into common practice. Across all cases, it is evident that crises push temporary fixes, but without binding rules, measurable capabilities, and practiced interoperability, advancements fail to become NATO norm. Unless corrected, the codification gap could reappear at the start of the next high-intensity conflict, when intelligence must be integrated suddenly rather than be already available.

Closing this gap means moving JISR towards a system that instills trust and capabilities to share. Four actions could foster this shift: write concrete ISR targets, create intelligence-readiness metrics, institutionalize annual JISR exercises, and adopt a tiered release policy. Together, these steps could likely align investments, create common sharing practices, and convert lessons from past operations into capability. Codification would not only strengthen operational capacity and promote a strategic posture, but by mandating, measuring, and exercising JISR, NATO could guarantee ISR integration that improves deterrence, enhances combat readiness, and replaces improvisation with reliability when it matters most.

Bibliography

Brattvoll, J. (2024, December 16). Intelligence disclosure as a strategic messaging tool. NATO Review. https://www.nato.int/docu/review/articles/2024/12/16/intelligence-disclosure-as-a-strategic-messaging-tool/index.html

Corbett, J., & Danoy, J. (2022, October 31). Beyond NOFORN: Solutions for increased intelligence sharing among allies. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-noforn-solutions-for-increased-intelligence- sharing-among-allies/

Davidson, J. (2025, June 5). What explains the transatlantic rift? It's all about threat perception. Atlantic Council. https://www.atlanticcouncil.org/blogs/new-atlanticist/what-explains-the-transatlantic-rift-its-all-about-threat-perception

Davis, G. B. (2023, March 16). The future of NATO C4ISR: Assessment and recommendations after Madrid. Atlantic Council. https://www.atlanticcouncil.org/in-depth-research-reports/report/the-future-of-nato-c4isr-assessment-and-recommendations-after-madrid/

Defense Innovation Board. (2024, July 10). Allies and Partners Study. U.S. Department of Defense. https://innovation.defense.gov/Portals/63/20240710%20DIB%20Allies%20and%20Partners%20Study%20FINAL.pdf

Freytag von Loringhoven, A. (2017, September 8). Adapting NATO intelligence in support of "One NATO". NATO Review. https://www.nato.int/docu/review/articles/2017/09/08/adapting-nato-intelligence-in-support-of-one-nato/index.html

Gilli, A., & Gilli, M. (2025, May). Appraising the state of play of C4ISR infrastructure within NATO: Gaps, deficiencies and steps forward. The Hague Centre for Strategic Studies. https://hcss.nl/wp-content/uploads/2025/05/Appraising-the-State-of-Play-of-C4ISR-Infrastructure-within-NATO-HCSS-2025-1.pdf

Gotkowska, J. (2013). NATO's intelligence, surveillance and reconnaissance: Gaps and needs. Centre for Eastern Studies (OSW). https://www.osw.waw.pl/en/publikacje/osw- commentary/2013-07-17/natos-intelligence-surveillance-and-reconnaissance-gaps-and

Grand, C. (2023, July 3). Defence spending: Sustaining the effort in the long-term. NATO Review. Retrieved from https://www.nato.int/docu/review/articles/2023/07/03/defence-spending-sustaining-the-effort-in-the-long-term/index.html

Greenleaf, J. R. (2013, March-April). The Air War in Libya. Air & Space Power Journal, 27(2). United States Air Force. Retrieved from https://www.airuniversity.af.edu/Portals/10/ASPJ/journals/Volume-27_Issue-2/F-Greenleaf.pdf

Haider, A., Menzel, M., & Perkins, W. (2015). Multinational Joint ISR Unit: A catalyst for NATO interoperability. Joint Air Power Competence Centre (JAPCC). https://www.japcc.org/wp-content/uploads/JAPCC_MJISRU_web.pdf

Horrell, S. (2022, July 1). NATO's Joint ISR and the Madrid Summit. Center for European Policy Analysis. https://cepa.org/article/natos-joint-isr-and-the-madrid-summit/

Huismans, J., Lucas, R., Palicka, O., Winder, S., & Silfversten, E. (2025). Conceptualising digital capability (RAND Research Report RRA-3831-1). RAND Corporation. https://www.rand.org/pubs/research_reports/RRA3831-1.html

International Institute for Strategic Studies. (2025). Progress and shortfalls in Europe's defence: An assessment – Introduction. IISS. https://www.iiss.org/publications/strategic-dossiers/progress-and-shortfalls-in-europes- defence-an-assessment/introduction

Jacobs, T. (2014). Conducting operations in a mission partner environment. Joint Force Quarterly, 72(1), 48–53. National Defense University Press. https://ndupress.ndu.edu/Media/News/News-Article-View/Article/577527/conducting-operations-in-a-mission-partner-environment/

Martin, M. J. (2014, January). Unifying Our Vision: Joint ISR Coordination and the NATO Joint ISR Initiative. Joint Force Quarterly, (72). National Defense University Press. Retrieved from https://ndupress.ndu.edu/Joint-Force-Quarterly/Joint-Force-Quarterly-72/Article/577482/unifying-our-vision-joint-isr-coordination-and-the-nato-joint-isr-initiative/

Murray, R. (2016, June). How NATO Makes the Unknown Known: A look at the improvements to NATO Joint Intelligence, Surveillance and Reconnaissance. Joint Air Power Competence Centre. Retrieved from https://www.japcc.org/articles/how-nato-makes-the- unknown-known/

NATO. (2016, July 7). Joint Intelligence, Surveillance and Reconnaissance (JISR). North Atlantic Treaty Organization.
https://www.nato.int/cps/en/natohq/topics_132685.htm

NATO. (2018). Unified Vision 2018 tests interoperability and new technologies. Retrieved from https://www.nato.int/cps/en/natohq/news_156098.htm?selectedLocale=en

NATO. (2025). AWACS: NATO's 'eyes in the sky'. North Atlantic Treaty Organization., https://www.nato.int/cps/en/natohq/topics_48904.htm

NATO. (n.d.). NATO Force Model. Retrieved from https://www.nato.int/cps/en/natohq/topics_234075.htm

North Atlantic Treaty Organization. (2012, May 20). Chicago Summit Declaration issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Chicago (Press Release 2012(062)). NATO.
https://www.nato.int/cps/en/natolive/official_texts_87593.htm

North Atlantic Treaty Organization. (2017, March 3). Joint Intelligence and Security (JIS) Division. NATO.
https://www.nato.int/cps/en/natohq/107942.htm

Riedenstein, C., Echikson, W., & Landrum, L. (2025, June). Defend in the cloud: Boost NATO data resilience. Center for European Policy Analysis (CEPA).
https://cepa.org/comprehensive-reports/defend-in-the-cloud-boost-nato-data-resilience/

Serena, C. C., Porche, I. R., Predd, J. B., Osburg, J., & Lossing, B. (2014). Lessons Learned from the Afghan Mission Network: Developing a Coalition Contingency Network (RR- 302). RAND Corporation.
https://www.rand.org/pubs/research_reports/RR300/RR302/RAND_RR302.pdf

U.S. Army War College. (2025, March 20). Measuring interoperability within NATO: Adapted off-the-shelf tool or bespoke solution?
https://publications.armywarcollege.edu/News/Display/Article/4129346/measuring-interoperability-within-nato-adapted-off-the-shelf-tool-or-bespoke-so/

F I N A B E L

THE EUROPEAN LAND FORCE
COMMANDERS ORGANISATION