ISBN 978-9934-619-28-1

Democratising Data Integration

Standardising Communication Protocols for Interoperable Data Processing and Analytics Tools in Strategic Information Environments

PREPARED AND PUBLISHED BY THE

NATO STRATEGIC COMMUNICATIONS CENTRE OF EXCELLENCE

ISBN: 978-9934-619-28-1

Authors: Hadley Newman, Dr Gundars Bergmanis-Korāts
Project Manager: Dr Gundars Bergmanis-Korāts
Content Editor: Hadley Newman
Design: Inga Ropša

DISCLAIMER
This report was completed in January 2025, based on interviews that were conducted throughout October and November 2024.

Riga, March 2025

NATO STRATCOM COE
11b Kalnciema iela,
Riga, LV1048, Latvia
stratcomcoe.org
@stratcomcoe

Democratising Data Integration

Standardising Communication Protocols for Interoperable Data Processing and Analytics Tools in Strategic Information Environments

Contents

Executive Summary

Data integration is an often-overlooked foundation of NATO's strategic communications, yet the challenge remains substantial due to highly fragmented implementation across systems and organisations. Without standardised data models, semantic structures, and API protocols, information exchange is delayed, hindering intelligence processing and impeding timely decisions.

This report underscores that the issue is not necessarily one of technology, effective tools already exist, but rather one of policy. Achieving seamless interoperability requires coordinated action, enforcement of standards, and the adoption of structured frameworks through well-defined policies that ensure consistent implementation across NATO allies and partners.

NATO's operational superiority depends on prioritising standardisation, governance, and innovation. Adopting AI-driven solutions enhances NATO's capacity to manage complex data environments, foster agility and resilience. Standardised communication protocols reduce complexity, improve efficiency, and strengthen security across integrated systems, particularly during crises when rapid and accurate data sharing is critical.

The report's recommendations highlight the importance of structured interoperability frameworks in enhancing institutional resilience, reducing procurement costs through efficient technology integration, and enabling coordination, improved response times, reduced workload and enhanced operational efficiency. Timely access to structured data ensures that NATO can respond swiftly to hostile narratives and dynamic operational challenges, reinforcing proactive communication strategies and safeguarding strategic coherence.

This report provides analysis and practical recommendations for establishing unified data standards, securing communication frameworks, and enabling multinational collaboration. It offers a clear pathway for NATO allies and partners to build resilient, cost-effective, and responsive data ecosystems that support sustained operational readiness and adaptability in an evolving information environment.

Introduction

The strategic communication discipline is evolving rapidly due to advancements in artificial intelligence, data analytics, and information-sharing platforms. A prominent development is the adoption of generative artificial intelligence models, offering extensive applications and significant value in data analytics. Their potential for data processing continues to attract attention[1,2,3,4], though precise prompting and fine-tuning remain resource-intensive, often requiring technical expertise. Integrating these models across multiple platforms presents challenges[5] such as biases in training data, varying performance for less widely spoken languages, and limitations in processing large volumes of information. Increasing reliance on AI for decision-making and analytics underscores the need for standardised data storage, sharing practices, and robust infrastructure across governments and organisations. As AI and data processing technologies evolve, organisations must address technical, ethical, and linguistic challenges to ensure operational effectiveness, compliance, and seamless integration within strategic communications.

Although not explicitly detailed in the report, these considerations are critical when evaluating the broader challenges of integrating artificial intelligence into strategic communications. In the long term, resolving technical, ethical, and linguistic issues is essential to ensuring AI adoption that aligns with operational effectiveness and compliance requirements.

In addition to advancements in data processing and generation technologies, the methods for accessing data are undergoing significant transformations. For example, European Union regulations have increasingly placed responsibility on social media platforms for data storage, sharing, and access. This regulatory framework has compelled platforms such as Twitter (now rebranded as X) to transition from being freely accessible research data facilitators to more commercially closed ecosystems[6]. Moreover, accessing social media data in hostile environments necessitates robust and secure mechanisms to protect sensitive information and ensure compliance with local laws. Equally critical is the need to harmonise and standardise data from diverse platforms, enabling seamless cross-platform data processing. Such integration is essential for comprehensive analytics and effective strategic communication, as it ensures consistency and interoperability across multiple data sources. Additionally, evolving access protocols and data governance standards require organisations to continually adapt to maintain data integrity and security. As the landscape evolves, staying informed about technological developments and regulatory changes will remain crucial for leveraging data effectively in strategic communications.[7]

A crucial reminder is that artificial intelligence is fundamentally reliant on data. Successful AI deployment requires standardised data storage and sharing practices across governments and organisations. Factors such as data modalities, file types, access restrictions, sharing capabilities, and user behaviours play pivotal roles in shaping the future of AI implementation. Additionally, the long-term integration and adoption of AI within large-scale government and institutional systems are inherently connected to the robustness of the underlying data infrastructure. This principle applies to defence, communication systems, and other sectors.[8,9]

Research Significance

Standardising communication *protocols*[10] is a critical strategy for addressing integration challenges and promoting interoperability. The adoption of standardised protocols reduces complexity, enhances efficiency, improves interoperability, and strengthens security across integrated systems. This approach is essential during crises, where the swift implementation of standardised protocols bridge capability gaps and support defence operations effectively. For example, the Russian war in Ukraine highlighted the vital importance of timely communication protocol adoption in the defence sector, enabling the rapid deployment of new systems and addressing existing vulnerabilities. Effective cross-government and cross-organisation data sharing relies on a collective understanding of data sources, structures, and the limitations involved in sharing, analysing, and decision making. Standardised communication protocols facilitate seamless data exchange by ensuring that all parties operate within a common framework, enabling accurate data interpretation and informed decision-making. This unified approach not only strengthens collaboration across diverse entities but also ensures data integrity and security throughout the integration process.

By adopting standardised communication protocols, organisations can enhance cohesion and responsiveness, resulting in more robust and resilient operational capabilities. Democratising data integration further empowers individuals at all organisational levels to access and analyse data, fostering informed decision-making. As data integration continues to evolve, organisations must proactively adopt emerging technologies and best practices. Remaining at the forefront of these developments is essential to effectively leverage data assets, address integration challenges, and support strategic decision-making.

Embracing a unified, standardised data integration strategy enables organisations to navigate the complexities of modern data environments, fully harness the potential of available resources, and ensure effective cooperation between governments during times of crisis.

Research Objectives

Integrating data tools in strategic communication requires a structured approach to address challenges and leverage opportunities. The report evaluates practices, addresses barriers, and outlines a path to enhance interoperability and efficiency.

The research focused on assessing existing methodologies, identifying technical and operational obstacles, developing a cohesive framework for standardised integration, and providing actionable recommendations to support implementation. These objectives underpin the analysis and findings presented, offering strategic insights to strengthen the capabilities of stakeholders operating in complex and dynamic environments.

The following objectives guided this report's analysis and recommendations:

1. Assess current integration methodologies
2. Identify key technical and operational barriers
3. Develop a framework for standardised data processing tool integration
4. Propose actionable recommendations for implementation

Methodology

A qualitative research approach was used to assess current integration methodologies, identify key technical and organisational barriers, and propose recommendations for integrating standardised data processing tools.

Research Design

A combination of qualitative expert interviews and comparative analysis was used to provide an in-depth understanding of current data integration challenges and potential solutions. Qualitative methods were chosen for their ability to capture nuanced insights from professionals with direct experience in strategic communications and data integration. Comparative analysis was applied to assess existing integration methodologies and identify best practices.

The expert interviews were conducted in strict confidence, ensuring a candid exchange of knowledge while maintaining the anonymity of participants. The selected interviewees included professionals with direct experience in data integration and strategic communication environments. These discussions provided first-hand perspectives on technological and organisational challenges, as well as potential pathways for enhancing interoperability. Due to the specialised nature of this research, qualitative interviews offered first-hand perspectives that could not be captured through quantitative analysis.

The comparative analysis examined existing integration methodologies, evaluating their effectiveness and applicability in different operational contexts. By reviewing established frameworks and industry practices, the research identified commonalities, gaps, and opportunities for improving cross-platform interoperability. This approach allowed for a structured assessment of how different methodologies align with strategic communication objectives.

Data Collection Methods

The research relied on two primary data collection methods:

Semi-structured expert interviews were conducted with professionals in data integration and strategic communications. These interviews followed a flexible format, allowing for deep exploration of key themes while ensuring consistency across responses. Given the confidential nature of the discussions, interviewee identities remain undisclosed.

Existing analytics tools were assessed through a **structured review of current technologies** used for data integration, identifying strengths and limitations in their ability to support interoperability across diverse systems.

Interoperability and Standardisation Frameworks

The integration of data processing tools in strategic communication and operational environments demands a robust foundation of technological standards. This section explores key interoperability and standardisation frameworks, evaluating their methodologies, applications, and comparative effectiveness in defence and civilian contexts.

Interoperability Frameworks

The methodologies underlying interoperability frameworks reflect the diverse requirements of military, governmental, and civilian organisations. These frameworks define how data is structured, processed, and exchanged across systems, ensuring seamless integration between allied forces and interagency stakeholders.

The **VAULTIS framework** provides a structured method for data integration, focusing on key areas such as visibility, accessibility, and security. These principles are critical in military operations, where data fluidity and secure information exchange are essential for real-time decision-making. The VAULTIS framework ensures that data remains both structured and accessible while mitigating risks associated with fragmented data systems.

For defence environments, **Federated Mission Networking (FMN)** serves as a cornerstone framework, designed to create a unified, multinational information-sharing network. FMN prioritises best practices for establishing a shared network that enhances collaboration across NATO allies and partners during joint operations. However, FMN's reliance on voluntary adoption poses challenges in ensuring full system integration across diverse national infrastructures.

Another significant NATO-driven framework is the **Data Integration and Analytics Framework (DIAT)**. DIAT is tailored for real-time data fusion, intelligence-sharing, and operational agility. By enabling interoperable data analytics tools, DIAT enhances situational awareness and decision-making efficiency, ensuring that military and governmental agencies can respond rapidly to emerging security threats[11].

In civilian and cross-border governance contexts, the **European Interoperability Framework (EIF)** and the **Interoperable Europe Act (IEA)** collectively provide a structured methodology for public sector interoperability. The EIF introduces four layers of integration, legal, organisational, semantic, and technical, ensuring structured cooperation between governments and intergovernmental entities. Semantic interoperability is particularly relevant for AI-driven automation and structured data processing in civil-military applications. Building on EIF, the IEA encourages cross-border compliance by introducing binding measures for interoperability standardisation, ensuring that EU member states and stakeholders follow a unified policy for digital interoperability[12]. The **Interoperable Europe Portal**, a key component of the IEA, serves as a collaborative repository for sharing integration tools, datasets, and best practices.

The **Open Data and Applications Government-owned Interoperable Repositories (Open DAGIR)** framework represents a government-led approach to data standardisation. Open DAGIR prioritises government

data ownership while fostering vendor collaboration, allowing for the secure integration of proprietary tools into military and civilian networks. It helps governments acquire and deploy software efficiently without being constrained by legacy systems or outdated procurement processes.[13] Open DAGIR's structured governance model helps mitigate vendor lock-in challenges and enhances procurement flexibility in defence environments.

Innovative interoperability solutions have gained traction: the **Delta Sharing protocol**[14] provides an open, standardised protocol for secure data exchange between multiple platforms, enabling cross-network collaboration without proprietary constraints. Meanwhile, **Data Clean Rooms**[15] introduce a controlled, privacy-enhanced environment for analysing shared datasets, ensuring secure collaboration while complying with regulatory requirements. These solutions offer scalable interoperability tools suited for civilian, governmental, and military data-sharing requirements.

Comparative Analysis

Across these frameworks, common themes emerge, particularly the prioritisation of semantic interoperability, data governance, and real-time analytics capabilities. However, key distinctions define their applicability in different contexts.

In military operations, FMN and DIAT complement each other by addressing different facets of interoperability. FMN facilitates multinational collaboration by establishing shared networks, while DIAT enhances operational agility through real-time data fusion and analytics. Despite their shared objective of improving situational awareness, FMN's voluntary adoption model poses integration challenges, whereas DIAT's structured approach ensures standardised analytical capabilities.

In the public sector, EIF and IEA provide complementary yet distinct approaches. While EIF offers flexible, voluntary guidance, IEA enforces mandatory compliance mechanisms, making it more effective for large-scale interoperability enforcement. The integration of the Interoperable Europe Portal into IEA further strengthens its ability to facilitate structured cooperation.

In government-controlled defence applications, Open DAGIR and VAULTIS provide secure, structured methodologies for data standardisation. Open DAGIR ensures that government-owned data repositories remain secure and adaptable, while VAULTIS focuses on enhancing data visibility and accessibility in structured environments.

Emerging technologies, such as Delta Sharing and Data Clean Rooms, bridge the gap between civilian and military needs, offering scalable, secure interoperability solutions. Their emphasis on data security and structured exchange mechanisms makes them suitable for cross-sectoral applications, particularly in scenarios requiring controlled access to shared datasets.

By leveraging these frameworks strategically, NATO allies and partners can achieve comprehensive interoperability, ensuring seamless data-sharing capabilities across military, governmental, and civilian environments.

Framework	Operational Scope	Core Functions	Strategic Importance	Adoption and Deployment
VAULTIS Framework	NATO and Allied Forces	Data visibility, accessibility, interoperability, and security	Critical for military operations requiring secure and seamless data flow	Structured methodology with military-specific data integration protocols
Federated Mission Networking	NATO allies and Partners	Multinational information sharing, secure network establishment	Enhances joint operations by enabling real-time, secure data exchange	Voluntary adoption across diverse national systems
Data Integration and Analytics Framework (DIAT)	NATO Alliance	Real-time data fusion, intelligence sharing, operational agility	Enables NATO-wide data analytics and decision-making capabilities	Tailored for military needs with structured integration mechanisms
European Interoperability Framework (EIF)	European Union	Legal, organisational, semantic, and technical interoperability	Foundation for cross-border public sector data sharing and service delivery	Voluntary guidelines for EU member states
Interoperable Europe Act (IEA)	EU-wide	Mandatory cross-border interoperabil-ity, structured cooperation	Strengthens cross-border digital services with enforceable standards	Mandatory assessments via the Interoperable Europe Board
Open DAGIR Framework	U.S. DoD and Government Agencies	Government-owned data repositories, vendor collaboration	Ensures secure data ownership and flexibility in military data procurement	Military-specific ecosystem with procurement and data governance focus
Delta Sharing Protocol	Global, Cross-Sector	Open protocol for secure data sharing across platforms	Supports civilian, governmental, and military collaboration without proprietary constraints	Open-source protocol enabling scalable interoperability solutions
Data Clean Rooms	Multinational, Cross-Sector	Privacy-enhanced shared data environments	Ensures secure, compliant data analysis in joint civilian-military operations	Controlled environments for regulated data collaboration
Information Exchange Framework (IEF)	NATO and Civil-Military Agencies	Policy-driven data-centric information sharing	Bridges policy and technical requirements for secure cross-agency data exchange	Policy and technology-aligned data-sharing protocols

TABLE 1. Summary of Interoperability and Standardisation Frameworks for Data Integration

Technical and Operational Barriers

Achieving seamless data integration across organisations remains hindered by several critical barriers, particularly in the realm of metadata standardisation. The United States Department of Defense's (US DoD) Metadata Guidance[16] underscores how metadata inconsistencies can lead to significant delays in operational decision-making, exacerbated by the diverse systems and tools employed across organisations, each with unique metadata schemas. Without a uniform approach to metadata management, interoperability remains constrained, increasing the risk of misinterpretation and inefficiencies in data processing workflows.

These challenges are particularly pronounced in Civil-Military Cooperation (CIMIC) contexts, where data-sharing between military, governmental, and civilian organisations is essential for effective crisis response, humanitarian aid coordination, and stability operations. The lack of standardised metadata frameworks across these sectors results in inconsistent data classification, delayed information exchange, and restricted access to critical operational intelligence. Without harmonised metadata structuring, CIMIC operations struggle to integrate civilian agency reports, NGO assessments, and military intelligence into a cohesive, actionable common operational picture.

The absence of structured metadata governance frameworks results in fragmented data classification, redundant data processing efforts, and difficulties in cross-organisational analysis. The lack of standardised metadata taxonomies prevents systems from accurately tagging and retrieving relevant data, leading to operational blind spots that can impair situational awareness. Additionally, manual metadata corrections are often required to align disparate systems, further slowing decision-making processes and reducing overall efficiency.

Compounding these challenges is the interplay between security classifications and metadata structures. Different organisations apply varying levels of data classification and tagging, often leading to restricted access or compatibility issues when attempting to share information across agencies. This lack of standardisation increases the likelihood of misaligned data security policies, creating additional layers of complexity for system interoperability and real-time information exchange.

Efforts to harmonise metadata structures across NATO allies as well as partners have been inconsistent and largely voluntary, resulting in a fragmented approach to metadata governance. The absence of a mandated, centralised metadata framework means that interoperability challenges persist, slowing the ability of organisations to leverage real-time analytics and intelligence-sharing mechanisms effectively.

One of the most pressing challenges to achieving interoperability across NATO allies and partners is the lack of standardised APIs (Application Programming Interfaces). Current data exchange systems often rely on proprietary APIs, leading to compatibility issues when integrating platforms from different

organisations. This fragmentation results in manual data transfers, increasing the risk of human error and slowing operational workflows. The absence of standardised APIs also limits the scalability of data-sharing systems, as new tools and platforms require custom integration solutions, further straining resources and operational timelines.

Additionally, security concerns associated with API integrations pose another barrier. Many organisations implement their own security protocols, making cross-platform API calls complex and potentially vulnerable. The need for consistent, secure APIs is essential, particularly in military contexts where real-time intelligence sharing is critical for mission success.

Assessment of Integration Challenges and Proposed Solutions

This section presents the research findings, identifying major integration challenges and introducing a proposed model for improving interoperability. The findings highlight technical barriers, organisational obstacles, and broader strategic factors affecting data integration in strategic communication environments. Additionally, the proposed integration model offers immediate, practical solutions while considering long-term strategic adaptations.

Integration Challenges

The research identified multiple challenges affecting the seamless integration of data across platforms, including technical limitations, organisational constraints, and broader strategic issues that impact interoperability efforts. Expert insights from interviews provided critical first-hand perspectives on these challenges, highlighting operational inefficiencies and areas requiring urgent intervention.

Technical Barriers

- **Lack of Standardised APIs**. Interviewees noted that “many NATO-affiliated organisations operate with proprietary or incompatible APIs, making integration across platforms cumbersome and resource-intensive.” The absence of standardised data-sharing protocols continues to be a major obstacle to interoperability.
- **Manual Data Transfer Processes**. Data sharing across the alliance and partners often relies on manual processes, such as CSV-based transfers. One expert described this as “a fundamental inefficiency,” explaining that “the reliance on manual data extraction and transfer slows down operations and increases the risk of human error.”

- **Scalability Limitations**. Existing infrastructure struggles to accommodate the increasing volume and complexity of operational data. “We are dealing with more data than ever before, but the systems we use are not designed to handle this level of complexity efficiently,” one interviewee stated.

- **Inconsistent Data Structuring**. Experts highlighted inconsistencies in how different NATO divisions structure their data. “A lack of unified metadata standards leads to compatibility issues, requiring additional time and resources for data cleaning and transformation,” explained one participant.

Organisational Obstacles

- **Divergent Institutional Protocols**. NATO allies and partners often operate with differing data-sharing protocols. One interviewee described this as “institutional inertia, each department has its own way of handling data and convincing them to change is a slow process.”

- **Limited Technical Expertise**. The absence of specialised expertise in data integration hinders the transition from outdated legacy systems due to knowledge gaps in implementing modern interoperability frameworks. “There’s a skills gap, some organisations are far ahead in automation, while others still rely on legacy manual input methods,” one expert noted.

- **Resource Constraints**. Budgetary limitations restrict organisations from investing in scalable and secure data integration infrastructures. “A lot of integration projects fail not because the technology isn’t there, but because there’s no long-term funding model to support them,” said one interviewee.

- **Data Privacy Considerations**. Compliance with data protection regulations such as GDPR complicates integration efforts. “We need to balance interoperability with legal obligations, especially in intelligence-sharing environments where regulatory constraints differ between partners,” an expert explained.

Proposed Approach to Integration

The findings highlight the need for a structured integration model that incorporates immediate practical solutions and long-term strategic considerations to enhance interoperability across diverse data environments. Expert interviews reinforced the importance of balancing operational efficiency with security and governance measures.

Standardisation Protocols

- **Unified Data Templating**. “A NATO-wide data model would simplify integration by ensuring all systems adhere to a common metadata standard,” suggested one interviewee.

- **Cross-Platform Compatibility Guidelines**. Experts stressed the need for interoperability frameworks that ensure tools used by different units can communicate seamlessly.

"Standardising data ingestion and API formatting across all strategic partners would be a game changer," one participant noted.

- **Security Compliance Frameworks**. Ensuring compliance with security protocols while maintaining operational agility is crucial. "We need a security-first approach that doesn't slow down data-sharing but still meets national and international cybersecurity requirements," explained an expert.

Technological Recommendations

- **API Development Standard.** Establishing mandatory API standards across NATO allies and partners would reduce integration complexity. "An open API framework could significantly improve real-time data exchange without compromising security," suggested an interviewee.

- **User-Friendly Interface Design**. Experts highlighted the need for more intuitive interfaces that reduce the reliance on manual data handling and provided the warning of: "One of the biggest barriers to adoption is usability, if the tools aren't easy to use, people will just default to the old methods," an expert warned.

- **Automated Data Processing Workflows**. "We should be leveraging AI-driven solutions for automated data classification and processing," an interviewee noted. Automating repetitive data integration tasks would enhance efficiency and reduce errors.

- **Training and Capacity-Building Strategies**. Experts emphasised the importance of continuous training. "Developing publicly accessible training materials on data interoperability would help bridge the skills gap across different units," one interviewee stated.

The proposed approach provides a roadmap for addressing immediate technical and operational challenges to integration while establishing the foundation for sustainable, long-term improvements in interoperability and data-sharing effectiveness. These insights, derived directly from industry professionals, reinforce the urgency of adopting structured, scalable, and secure data integration strategies.

Practical Implications

The integration of standardised data processing and interoperability frameworks has profound implications for organisations operating in strategic communication and defence environments. Beyond technological advancements, the success of these initiatives hinges on their operational and policy-level implementation. This section examines how improved interoperability influences strategic communication effectiveness, enhances organisational efficiency, and supports policy-driven decision-making.

Strategic Communication Enhancement

The ability to seamlessly integrate and analyse data across platforms strengthens an organisation's strategic communication capabilities. Standardised data-sharing protocols enable more efficient threat detection, comprehensive risk assessments, and rapid response strategies. Improved interoperability enhances the capacity to track and analyse narratives in real time, allowing organisations to identify emerging disinformation campaigns and coordinate countermeasures more effectively. One expert noted, "**Timely access to structured data allows us to respond to hostile narratives before they gain traction, reinforcing proactive communication strategies.**"

From an operational perspective, improved data integration enhances situational awareness by ensuring access to accurate, cross-verified information. This is particularly critical in defence, where decision-making depends on the ability to aggregate intelligence from diverse sources. Effective interoperability reduces information silos, enabling rapid data-sharing that enhances synchronised threat-response operations.

Organisational Benefits

At the institutional level, adopting standardised integration frameworks results in measurable efficiency gains. The automation of data workflows reduces the time spent on manual data processing and minimises errors associated with fragmented data-sharing practices. One interviewee observed, "**Eliminating redundant data entry and conversion processes has significantly improved response times and reduced workload.**"

Enhanced interoperability also facilitates cross-institutional collaboration by providing a shared data environment where multiple stakeholders can operate efficiently. A unified approach to data integration reduces duplication of effort and fosters alignment between different departments and partners. "Interoperability isn't just about technology, it's about creating an ecosystem where agencies can function as a cohesive unit," explained one expert.

Financially, **improved data-sharing protocols contribute to cost-effective technology integration**. **Minimising reliance on proprietary systems reduces procurement costs and long-term maintenance expenses associated with repeated software modifications.** Moreover, increased automation and improved data accessibility enable personnel to focus on high-value analytical tasks rather than time-consuming administrative functions.

Beyond measurable operational improvements, the **adoption of structured interoperability frameworks enhances institutional resilience**. Organisations that implement

robust integration strategies are better positioned to adapt to evolving threats, regulatory changes, and shifts in the information environment. By ensuring proactive governance, these frameworks ensure long-term sustainability and agility in strategic communication operations.

Recommendations

To improve interoperability and standardised data integration, these recommendations address operational, policy, and technological needs, ensuring organisations can enhance their data-sharing capabilities while maintaining security and compliance.

Short-Term Interventions

To address immediate interoperability challenges, several short-term measures should be implemented to standardise metadata practices and improve data-sharing across NATO and partners:

- **Develop and Implement a NATO-Wide Metadata and API Framework:** Establish a standardised metadata and API model aligned with NATO and US DoD standards to ensure structured classification, tagging, and consistent data exchange across systems.
- **Deploy Automated Validation Tools:** Integrate automated metadata and API validation tools to detect and correct inconsistencies in real time, improving data accuracy and reducing manual processing inefficiencies.
- **Integrate CIMIC Standards:** Facilitate civil-military interoperability by ensuring metadata and APIs used by governmental bodies, NGOs, and military forces adhere to a unified structure.
- **Enhance Training and Awareness:** Expand training programmes to include metadata and API standardisation practices, equipping personnel to maintain consistent data classification, structuring, and secure API usage.
- **Establish a Compliance Mechanism:** Introduce mandatory compliance mechanisms to ensure all partners adhere to metadata and API standards, mitigating fragmentation.

Foundational Steps for Long-Term Strategies

While short-term interventions provide immediate improvements, a structured long-term approach is necessary to ensure standardisation remains effective:

- **Create an Interoperability Governance Body:** Establish a centralised body to oversee metadata and API standardisation policies, ensuring sustained compliance and integration across evolving landscapes.
- **Develop Cross-Sector Alignment Protocols:** Align military, civilian, and governmental data structures and APIs for seamless data fusion among stakeholders.
- **Integrate Standards into Cybersecurity Frameworks:** Embed metadata and API governance within security protocols to ensure consistent access control and data security.
- **Facilitate Multinational Standardisation Agreements:** Establish agreements for consistent metadata taxonomy and API usage across NATO and non-NATO allies.

Strategic Direction

Sustainability in metadata governance requires a strategic approach to ensure interoperability, adaptability, and resilience in evolving information environments:

- **Invest in AI-Driven Metadata and API Structuring:** Explore AI-powered tools for dynamic metadata tagging and API management adaptable to new data formats and operational needs.
- **Establish Research Initiatives:** Launch dedicated programmes to evaluate future metadata and API frameworks, ensuring alignment with technological advancements.
- **Strengthen CIMIC Data-Sharing Capabilities:** Prioritise metadata and API solutions for real-time data exchange between military and civilian actors.
- **Develop Resilient Policies:** Continuously review and update metadata and API standards to address emerging cyber threats, hybrid warfare, and adversarial risks.

These recommendations provide a roadmap for achieving effective interoperability by addressing both short-term constraints and long-term strategic priorities. By implementing these measures, organisations can build a resilient and adaptable data integration ecosystem.

Proposed Integration Model – API Development Standards

An effective integration model for API development within NATO must incorporate a tiered approach, categorising APIs based on sensitivity, operational requirements, and system compatibility. The proposed model includes:

- **Baseline API Standards** for general data exchange across NATO operations, ensuring all systems use common protocols, aligned with mandatory interoperability profiles and technical standards outlined in ADatP-34 NATO Interoperability Standards and Profiles (NISP)[17].

- **Secure API Standards** incorporating multi-factor authentication incorporating multi-factor authentication, encryption, and zero-trust principles, as emphasised in the United States Department of Defence's Application Programming Interface (API) Technical Guidance[18], which highlights the need for robust security frameworks and continuous monitoring for early threat detection.

- **Specialised API Standards** for high-demand operations, prioritising low-latency and high-security communications, reflecting recommendations by Office of the Executive Director for Systems Engineering and Architecture/ Office of the Under Secretary of Defense for Research and Engineering[19] on optimised API performance and seamless system integration under operational stress.

Automated validation tools should be embedded into development lifecycles to ensure compliance with NATO standards, with conformance criteria and key performance indicators provided in ADatP-34 NISP for validating service interoperability points. Modular API designs should be prioritised, offering reusable components across different platforms to reduce costs and integration timeframes, aligning with the API Technical Guidance's emphasis on composability and reuse for operational efficiency.

Additionally, the integration model must support dynamic API management through DevSecOps practices, continuous testing, and real-time adaptability, ensuring APIs remain resilient and scalable across evolving NATO operational needs. This model ensures NATO allies and partners achieve seamless, secure, and scalable data integration, enhancing operational readiness and cross-platform interoperability through adherence to established API development and interoperability standards.

Limitations and Future Research

Limitations

While this report provides valuable insights into the challenges and solutions related to data integration and interoperability, several practical constraints have influenced the scope and applicability of the findings.

- **Institutional Resistance to Change**. A significant barrier to implementing standardised interoperability frameworks is the reluctance of organisations to modify existing processes. Institutional resistance and misaligned organisational priorities delay the adoption of new technologies and standardised frameworks.

- **Geopolitical and Regulatory Complexities**. Data-sharing initiatives across multiple jurisdictions face legal and regulatory challenges. Variations in data protection laws, including the stringent requirements of GDPR in European contexts compared to differing regulatory approaches in non-EU states, create obstacles to seamless integration.

- **Funding and Resource Allocation**. Many organisations, particularly within governmental and military settings, operate under budget constraints that limit their ability to invest in modern data integration solutions. Legacy systems remain in place due to the high costs associated with transitioning to newer technologies.

- **Security Concerns**. The need to maintain robust cybersecurity postures often leads to restrictive access controls, complicating efforts to create open and interoperable data environments. Risk-averse institutions may delay or limit participation in broader interoperability initiatives to safeguard classified or sensitive information.

- **Technology Disparities Among Partners**. Varying levels of technological maturity among stakeholders create inconsistencies in implementation. While some institutions have advanced automation and data-sharing capabilities, others still rely on manual data transfers, limiting overall interoperability efforts.

These limitations highlight the complexities involved in achieving seamless integration and underscore the importance of tailoring interoperability solutions to the specific constraints of participating institutions.

Future Research Trajectories

To address these challenges and further develop effective data integration solutions, future research should prioritise applied studies.

- **Longitudinal Studies on Integration Effectiveness**. Future research should assess the long-term impact of interoperability frameworks by tracking effectiveness over extended periods. This would help determine whether implemented solutions achieve sustained improvements in data-sharing efficiency and security.

- **Advanced AI-Driven Integration Methodologies**. While AI-powered solutions are already being explored, further research is needed to evaluate the role of machine learning models in automating data categorisation, enhancing metadata standardisation, and improving real-time interoperability.

- **Cross-Sectoral Case Studies**. Examining successful interoperability initiatives across different sectors, such as finance, and intelligence, could provide valuable lessons for defence and strategic communication environments.

- **Scalability and Adaptability of Interoperability Frameworks**. Future studies should explore the flexibility of existing frameworks in adapting to emerging technologies, ensuring that integration models remain relevant as new challenges arise.

- **Cybersecurity and Risk Management Strategies**. Given ongoing security concerns, research should investigate best practices for balancing interoperability with data protection. This could include studies on encrypted data-sharing models, zero-trust architectures, and secure learning approaches.

By pursuing these priorities, organisations and policymakers can refine existing frameworks and develop more adaptable, resilient interoperability solutions that align with evolving technological and security landscapes.

Conclusion

This report has examined the critical challenges and opportunities associated with data integration and interoperability within strategic communication and defence environments. It has highlighted the technical and organisational barriers that impede seamless data-sharing, including the lack of standardised APIs, inconsistent data structuring, institutional resistance to change, and geopolitical constraints. The findings underscore the importance of adopting structured integration models that balance security, efficiency, and cross-platform compatibility.

By implementing standardisation protocols, organisations can establish unified data frameworks that ensure consistency across systems. The development of interoperable technologies, such as automated data workflows and user-friendly integration solutions, offers immediate practical benefits while setting the foundation for long-term adaptability. Addressing organisational and institutional challenges through enhanced governance, improved procurement policies, and targeted capacity-building initiatives will further strengthen the effectiveness of data-sharing mechanisms.

Beyond these technical and operational considerations, the broader significance of this research lies in its contribution to policy development and institutional resilience. By fostering multinational collaboration and establishing compliance-driven integration frameworks, organisations can enhance their ability to respond to emerging security threats and evolving information environments. The findings reinforce the need for sustained investment in technological advancements while ensuring that integration strategies remain aligned with shifting regulatory and geopolitical landscapes.

To maintain operational superiority and strategic coherence, NATO and partners must prioritise **standardisation, governance, and innovation, while embracing AI-driven solutions** as core elements of their interoperability efforts. **Standardisation** establishes a unified approach to data structuring, ensuring seamless cross-platform integration and enabling multinational forces to maintain a shared, real-time operational picture. **Without universally accepted data models, semantic structures, and API protocols, information exchange remains fragmented, creating unnecessary delays in intelligence processing and decision-making.**

Governance plays an equally vital role in ensuring that integration efforts adhere to security, legal, and ethical standards. Establishing strong oversight mechanisms, compliance frameworks, and regulatory coordination will enable NATO to mitigate risks associated with data sovereignty, cybersecurity vulnerabilities, and institutional misalignment. As defence alliances continue to operate in an increasingly complex digital ecosystem, structured governance ensures integration initiatives do not compromise national security interests while fostering trust among partners and mitigating technical barriers to seamless integration.

Finally, **innovation** must be embedded within NATO's long-term data strategy to maintain technological agility and adaptability. The rapid evolution of artificial intelligence, quantum computing, and cloud-based analytics necessitates a forward-thinking approach that embraces emerging capabilities while mitigating associated risks. Investing in research and development, piloting automated solutions, and leveraging AI-driven data structuring will be key to ensuring that interoperability efforts remain future-proof. Without sustained innovation, NATO risks technological obsolescence, leaving its strategic communication and defence coordination efforts vulnerable to adversarial advancements.

Looking ahead, the challenges associated with data interoperability will continue to evolve as new technologies emerge and security requirements become increasingly

complex. Future efforts should focus on refining existing frameworks, leveraging AI-driven methodologies for enhanced automation, and ensuring that interoperability remains a priority in cross-agency and international cooperation. As organisations adapt to these developments, a commitment to standardisation, governance, and innovation will be essential to achieving long-term success in strategic communication and data integration.

We recognise that policy adoption across organisations is challenging. Implementation between governments and across nations is inherently complex, even though the technology to enable secure, enduring, and efficient data governance is already available. So, what must be done now? Establishing standardised APIs for information acquisition and analysis is a critical step towards strengthening the resilience and readiness of the defence sector in anticipation of future crises. However, the adoption of standardised APIs must not be seen as an endpoint. Rather, it should serve as the foundation for advancing interoperability, institutionalising standardised information exchange formats, and embedding a cohesive, enduring approach to data and information governance across the Alliance and partners.

Endnotes

1 Henke, J. (2024). Navigating the AI era: university communication strategies and perspectives on generative AI tools JCOM 23(03), A05. *https://doi.org/10.22323/2.23030205*

2 Klein-Avraham, I., Greussing, E., Taddicken, M., Dabran-Zivan, S., Jonas, E. and Baram-Tsabari, A. (2024). How to make sense of generative AI as a science communication researcher? A conceptual framework in the context of critical engagement with scientific information JCOM 23(06), A05. *https://doi.org/10.22323/2.23060205*

3 Gans, J. S. (2024). How will Generative AI impact communication?. *Economics Letters*, 242, 111872.

4 Arthur W. Page Society. (2024, November 22). From Efficiency to Impact: How GenAI is Transforming Communications Strategy - Arthur W. Page Society. Arthur W. Page Society - Page & Page up Unite the World's Best Communicators to Transform Business for the Better. *https://page.org/knowledge-base/from-efficiency-to-impact-how-genai-is-transforming-communications-strategy/*

5 Bergmanis-Korāts, G., Bertolin, G., Pužule, A., Zeng, Y. AI in Support of StratCom Capabilities. Riga: NATO Strategic Communications Centre of Excellence

6 Killeen, M., & Böswald, L. (2023, February 21). Why Twitter's decision to charge for data access could risk EU fines. Euractiv. *https://www.euractiv.com/section/digital/opinion/why-twitters-decision-to-charge-for-data-access-could-risk-eu-fines*

7 A guide to the Digital Services Act, the EU's new law to rein in Big Tech - AlgorithmWatch. (n.d.). AlgorithmWatch. *https://algorithmwatch.org/en/dsa-explained*

8 Graux, H., Gryffroy, P., Gad-Nowak, M., Boghaert, L., & European Commission. (2024). The role of artificial intelligence in processing and generating new data: An exploration of legal and policy challenges in open data ecosystems. Publications Office of the European Union. *https://data.europa.eu/sites/default/files/report/The%20Role%20of%20Artificial%20Intelligence%20in%20Processing%20and%20Generating%20New%20Data-1-2.pdf*

9 Bergmanis-Korāts, G., Bertolin, G., Pužule, A., Zeng, Y. AI in Support of StratCom Capabilities. Riga: NATO Strategic Communications Centre of Excellence

10 In this report "communication protocols" refer to concepts & frameworks of standardised information acquisition, storage & sharing across entities

11 Summary of NATO's Data Exploitation Framework Strategic Plan, NATO, *https://www.nato.int/cps/fr/natohq/official_texts_209999.htm?selectedLocale=en*

12 European Interoperability Framework. (n.d.). Interoperable Europe Portal. *https://interoperable-europe.ec.europa.eu/collection/nifo-national-interoperability-framework-observatory/european-interoperability-framework*

13 Chief Digital and Artificial Intelligence Office. (n.d.). Chief Digital and Artificial Intelligence Office > Initiatives > Open DAGIR. *https://www.ai.mil/Initiatives/Open-DAGIR/*

14 *delta.io/sharing*

15 *iabtechlab.com/wp-content/uploads/2023/02/FINAL-DRAFT-PUBLIC-COMMENT-Data-Clean-Room-Guidance-IAB-Tech-Lab.pdf*, *databricks.com/product/clean-room*

16 US DoD Data Strategy: *https://www.ai.mil/Portals/137/Documents/Resources%20Page/DoD%20Metadata%20Guidance.pdf*

17 *https://live.nisp.nw3.dk/pdf/NISP-v14.pdf*

18 *https://www.cto.mil/wp-content/uploads/2024/08/API-Tech-Guidance-MVCR1-July2024-Cleared.pdf*

19 *https://www.cto.mil/wp-content/uploads/2024/05/API-Guide-2023.pdf*

Prepared and published by the
NATO STRATEGIC COMMUNICATIONS
CENTRE OF EXCELLENCE

The NATO Strategic Communications Centre of Excellence (NATO StratCom COE) is a NATO accredited multi-national organisation that conducts research, publishes studies, and provides strategic communications training for government and military personnel. Our mission is to make a positive contribution to Alliance's understanding of strategic communications and to facilitate accurate, appropriate, and timely communication among its members as objectives and roles emerge and evolve in the rapidly changing information environment.

www.stratcomcoe.org | @stratcomcoe | info@stratcomcoe.org