AI & SOCIETY (2026) 41:1131–1148
https://doi.org/10.1007/s00146-025-02610-5

OPEN FORUM

Ethical, legal, and social challenges of data economy in defence the case of battlefield data

Brian Kot[1] · **Jack Burling Nebe**[1] · **Mariarosaria Taddeo**[1]

Received: 7 April 2025 / Accepted: 6 September 2025 / Published online: 22 September 2025

Abstract
Battlefield data have become a critical asset in contemporary defence. Yet there is a gap in the relevant literature, whilst it addresses various aspects of defence data management—including cybersecurity, interoperability, and decision-making support—it overlooks how these data should be collected, curated, and accessed to enhance the responsible development of AI-enabled defence capabilities. This article addresses this gap first by reviewing existing data policies strategies of NATO and Five Eyes Member States to assess the extent to which they focus on battlefield data, and then by outlining how national defence organisations should manage these data to maximise their strategic value whilst mitigating the attendant ethical, legal, and social risks. We argue that due to their non-rivalrous, artificially excludable nature, battlefield data should be conceptualised as an *artificial club good* and that national defence organisations have ethical obligations to act as *club manager* to leverage the potential of these data to develop more robust, reliable and controllable AI defence capabilities. We conclude the analysis proposing two sets of policy recommendations to aid national defence organisations in discharging their responsibilities as club managers for battlefield data.

Keywords Artificial intelligence, AI Ethics · Battlefield data · Data-centric defence · Data governance · Data sovereignty · Defence · Defence digitalisation · Defence technology, Ethics of Defence

1 Introduction

The use of data to improve defence capabilities is not a novelty in defence. For instance, the Patriot missile systems have long collected data on interception accuracy and overall effectiveness, informing refinements in air defence strategies.[1] Companies, such as Lockheed Martin, Northrop Grumman, and BAE Systems, integrate secure telemetry systems in their technologies, ensuring that defence stakeholders receive comprehensive performance insights. However, the digitalisation of defence—the increasing reliance of defence processes on digital technologies—and the adoption of defence capabilities endowed with artificial intelligence (AI) have made data essential. With AI, data have become an increasingly strategic asset in defence (Taddeo 2024).

Literature on the management of defence data is vast, and key themes include cybersecurity risks, interoperability within national forces and amongst alliances, readiness of access, and how to leverage data to support decision-making. To the best or our knowledge, in this debate, however, there is little specific and explicit focus on *battlefield* data and how they should be managed—collected, stored, and shared—to support defence, whilst avoiding ethical, legal, and social risks. This article fills this gap, by considering how national defence organisations (i.e. ministries of defence, defence procurement agencies, defence research institute, defence forces, defence and review board) can, and ought to, leverage the potential of battlefield data to support the development of AI defence technologies.

Filling this gap has become increasingly more important as digital technologies are becoming pervasive in defence. Historically, collection and management of battlefield data were predominantly within the purview of governmental defence agencies. However, the adoption of digital

✉ Mariarosaria Taddeo
mariarosaria.taddeo@oii.ox.ac.uk

Brian Kot
brian.kot@politics.ox.ac.uk

Jack Burling Nebe
jackburlingnebe@gmail.com

[1] Oxford Internet Institute, University of Oxford, Oxford, United Kingdom

[1] https://www.gao.gov/assets/t-nsiad-92-27.pdf.

technologies, and particularly AI, has propelled private technology companies to the forefront of data collection, management, and analysis. This transition is evident in various facets of defence operations, including intelligence gathering, surveillance, and reconnaissance (Blanchard and Taddeo 2023; Ghioni et al. 2024) (). And it can have severe negative ethical, legal, and social implications (ELSI), like the erosion of data sovereignty, breaches to privacy, and hindering the development of more robust and reliable technological defence capabilities. Here, we argue that we should shift from a private-led to a public-led curation of these data and that defence agencies have obligations—that is an obligation that follows them being part of a State—to play a more active role in the collection and management of these data and to leverage them to support the development of more robust AI technologies. We also note that the analysing and addressing ethical challenges posed by battlefield data has implications that extend beyond these specific data to the broader digitalisation of defence technology, making battlefield data governance a crucial test case for wider defence sector data policies.

In the rest of this article, we take battlefield data to indicate data collected within, or about, battlespace activities, conditions, and adversarial operations. They comprise, amongst other things, terrain and weather data, locations, movement of combatants, non-combatant data electronic warfare, cybersecurity on the battlefield, strategic analysis, logistics, supply chain, and infrastructure, systems performance. The volume of these data has increased dramatically over the past decades thanks to the adoption of a host of digital technologies in defence. For example, progress in the miniaturization of computing power has increased the availability of high-fidelity sensors deployed on the battlefield (Watling 2023). Machines can now pick up, store, and process a widened range of signals—radar, electro-optical, acoustic, electromagnetic, thermal and positional—about the battlespace (Zhu et al. 2021).[23]

Compared with the controlled, often digital, environments (e.g. social media, finance, insurance, medicine, manufacturing and gameplay), battle environments are often devoid of complete, high-quality, non-discrepant data, because such environments are harsh, adversarial, complex and variable (Michel 2023). Developing AI on such highly complex and variable data improves the robustness of these technologies, their reliability, and may even foster better human control. For example, as a standard business practice, a drone company operating in a warzone regularly logs its drones' flight data. The battle environment would likely leave imprints onto these data, by recording any disruptions to the data link between the drone and its operator arising from adversarial electronic warfare. These data can offer insights on how to improve the drones' performance in such an environment. A common tactic against drones is jamming electronic signals. Drone developers that could rely on data about flying whilst being jammed can keep improving their drones so that they can operate in other challenging, adversarial environments (Meaker 2023).

In this article, we offer a review of the relevant policies strategies to evaluate their focus on battlefield data (Sect. 2). We then outline the principal ethical challenges associated with managing such data, ranging from the privatisation of battlefield data and the erosion of data sovereignty to heightened risks of privacy breaches and mass surveillance (Sect. 3). We proceed to present our conceptual framework for a defence-led management of battlefield data, showing how this framework enables defence organisation to addresses effectively several of these challenges outlined in Sect. 3 and to meet their ethical obligations (Sect. 4). Finally, we offer two sets of policy recommendations aimed at maximising the strategic value of battlefield data for defence (Sect. 5). The Annex complements this analysis by detailing four primary approaches to data management in defence, along with their ethical and security implications.

2 Mapping Data-centric defence policies

We reviewed relevant policies of Western defence actors (we focussed on Five Eyes' and NATO's Member States and of NATO itself) to assess the extent to which they address specifically battlefield data and their use to support development of AI technologies. We find that existing policies prioritise using data to improve real-time decision-making and enhance networked warfighting capabilities—primarily through data interoperability and shared standards for data quality and curation. When considering battlefield data specifically, our analysis shows that all reviewed Western defence organisations recognise the value of these data, but only Germany, the UK, and the US have published policies to exert some form of control over these data. Of the three countries, only the US has defined policies to leverage the potential of these data to develop and improve AI technologies (Table 1). This approach, however, remains severely undermined by questions concerning the protection of intellectual property (IP), more on this presently.

[2] The reader interested in more information, may find useful visiting this link for detailed list of parameters for drone-enabled data collection https://ardupilot.org/plane/docs/logmessages.html.

[3] In the rest of this article we use 'defence data' to refer to all data related to defence activities, not only those related to battlefield. We use 'battlefield data' to indicate specifically data as defined in this section.

Table 1 A summary of the key finding of our review of data governance policies of Five Eyes', NATO's Member States, and of NATO itself

State actor	Data strategy focus	Battlefield data management	AI development support	Key limitations
Australia	Real-time battlefield analytics across domains via Joint Data Network	No specific management policies	Limited emphasis on AI innovation	Focus on battlespace understanding rather than technological innovation
Canada	Comprehensive data governance framework (DAOD 6500-0)	No specific management policies	Decision-making focus only	Primary use for operational advantage, not R&D
France	SCORPION programme for real-time information sharing	No specific management policies	Lacks R&D integration	Strategic documents present but missing battlefield data specifics
Germany	AI coordination for C4ISR and joint-domain operations	Limited (SFCAS programme only)	Limited (proof of concept)	Contractors required to supply data via centralised platform for SFCAS only
New Zealand	Information management programme for data modernisation	No specific management policies	No AI development support	Focus on digital literacy and enterprise systems
Spain	European defence fund participation	No specific management policies	No technology development	Data sharing with NATO allies for analysis only
United Kingdom	Data strategy for defence treating data as strategic asset	Partial framework established	Unspecified AI support	Contractor data-sharing protocols exist but lack AI development specifications
United States	Comprehensive data initiatives including federated catalogues	Most advanced approach	Yes, but undermined	IP protection issues severely limit effectiveness of 2023 AI Adoption Strategy
NATO	Alliance data-sharing ecosystem pilot initiative	No specific management policies	Unclear future direction	Federation model for interoperability, AI development potential uncertain

2.1 Data management policies across western defence organisations

The Australian Department of Defence has adopted a battlefield data strategy through its Joint Data Network initiative, focussing on integrating real-time battlefield analytics across land, sea, air, and cyber domains (Department of Defence 2024a). The Department's Defence Data Strategy 2021–2023 and the updated Defence Strategy 2.0 stress the decision advantage achieved by transitioning to a data-centric defence force (Department of Defence 2021). Central to the implementation of the data strategies is the OneDefenceData platform, which provides a common interface linking disparate data sources to enable enterprise-wide data catalogues, archiving, search, access, and analytics, bringing together a reliable and accurate common operating picture (Department of Defence 2024b). In these documents, the primary function of data is to facilitate greater understanding of the battlespace; there is less emphasis on using data as a key input to defence technological innovation.

The Canadian Department of National Defence and the Canadian Armed Forces have also established a comprehensive policy approach for the collection, sharing, and management of battlefield data. These initiatives aim to enhance operational effectiveness and ensure that data is leveraged as a strategic asset. One of the key policies in this area is the Defence Administrative Orders and Directives 6500-0[4] on Data Management and Analytics. It focuses on enabling authorised personnel to access, collect, and manage data across all defence programmes, supporting a data governance framework that defines the roles of data stewards, ensuring data interoperability with allies, and maintaining data quality and security (Department of National Defence and Canadian Armed Forces 2022). The 2019 DND/CAF Data Strategy envisions data to be leveraged in "all aspects of Defence programmes", but the primary use case remains focussed on "enhancing our defence capabilities and decision-making, and providing an information advantage during military operations" (Minister of National Defence 2019, 9).

The French Ministry of Armed Forces has advanced battlefield data collection through its SCORPION programme.[5]

[4] https://www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/6000-series/6500/6500-0-data-management-and-analytics.html.

[5] https://www.army-technology.com/news/scorpion-vehicles-jaguar-and-griffon-delivered-to-the-french-army/#:~:text=counter%2Ddrone%20landscape-,SCORPION%20vehicles%2C%20Jaguar%20and%20Griffon%2C%20delivered%20to%20the%20French%20Army,time%20communication%20and%20battlefield%20digitisation.

This programme focuses on modernizing the French Army's capabilities by integrating real-time information sharing across armoured vehicles, command centres, and infantry units. A central component of SCORPION is the *Système d'Information du Combat de SCORPION*, that facilitates collaborative combat through real-time communication and battlefield digitization. In line with NATO's approach, French defence policies prioritise interoperability with NATO allies and relies on structured data-sharing agreements with contractors to refine combat operations. The French Ministry of Armed Forces has published a series of strategic documents—including the 2018 Digital Transformation strategy, the 2019 AI in Support of Defence Strategy, and the 2021/2023 Data Roadmap—to prioritise the use of data for gaining operational superiority (Martin and Liversain 2024). These are much-needed steps to modernising the French defence's data governance, yet they lack a precise description for how battlefield data should be managed and leveraged for the research and development of defence technological capabilities.

Germany's Bundeswehr prioritises the use of data in enabling seamless combat operations. For instance, the Army has published a series of concept notes outlining its vision for the future digital battlefield, emphasising the use of AI to coordinate a growing number of sensors and effectors and improve capabilities across Command, Control, Computers, and Communications and Intelligence, Surveillance, Reconnaissance (C4ISR). The Luftwaffe, too, expects AI to synchronise data to enable joint-domain operations (Borchert et al. 2024). This approach is exemplified by the European *Système de Combat Aérien Futur* (Future Combat Air System) (SFCAS) programme. SFCAS is an interesting example of a shift in data management in defence. It involves Germany, France, and Spain, and aims to develop a sixth-generation advanced combat aircraft by 2040. The programme emphasizes the collection of battlefield data through advanced sensor fusion and AI-enabled combat analysis. Contractors working with the German defence are required to supply operational data to users via a centralised platform to enhance system performance and maintain compatibility with European defence initiatives.[6] This is a cautious step in the right direction with respect to leveraging the potential of data for technological innovation. Albeit limited to the development of a specific capability, this programme may serve as a proof of concept for any strategies attempting to leverage in a systemic way the potential of battlefield data to develop AI-enabled defence capabilities.

[6] https://thedefensepost.com/2024/06/12/german-consortium-ai-backbone/#:~:text=A%20consortium%20of%20German%20firms,the%20German%20armament%20procurement%20agency.

The New Zealand Defence Force (NZDF) has now devised an Information Management Programme to modernise its data management practices. Some of the programme's deliverables include the creation of an integrated data platform, an enterprise digital archive, and general programmes to enhance digital literacy across the defence force (Little 2023). At the operational level, in line with the New Zealand Defence Doctrine, the NZDF acquired SitaWare Command & Control and Battle Management System, which provides a comprehensive view of the battlefield, enabling rapid information sharing amongst headquarters, units, vehicles, and individual soldiers ('New Battle Management Software for the Army' 2016). Yet, there are no measures addressing explicitly the collection and use of battlefield data to support AI, or wider technology, development.

The Spanish Armed Forces have invested in battlefield data-sharing technologies as part of their participation in the European Defence Fund. Data collection from Spanish uncrewed aerial vehicles and armoured divisions is transmitted to NATO allies for joint analysis and operational improvement (Martin 2023). However, Spanish policies recognise the strategic importance of battlefield data, their primary focus remains on interoperability rather than leveraging these data to foster more robust, secure, and reliable defence technologies, particularly AI-driven ones.

The UK Ministry of Defence (MOD) has articulated a comprehensive approach to data management through its Data Strategy for Defence, emphasising the treatment of data as a strategic asset (UK Ministry of Defence 2021). The strategy mandates that all defence-related data to be collected, curated, and exploited across governmental departments to enhance decision-making capabilities and operational efficiency. A notable aspect of this strategy is the establishment of data-sharing protocols that defence contractors are required to adhere to. These protocols ensure that pertinent data from various defence activities are accessible to relevant stakeholders within the MOD, fostering a more integrated defence infrastructure. The MOD has also established frameworks and regulations that require defence contractors to share data related to their testing environments, including battlefield data from drone testing. These measures heading in the right direction. However, they offer a partial solution to the questions of management of battlefield data, insofar as they do not specify whether these data can, or indeed should, be leveraged to support the development of new AI capabilities.

The UK Data Strategy for Defence also establishes a framework for data management. Through data-sharing protocols and comprehensive cybersecurity requirements, the MOD ensures that defence contractors contribute to the defence data ecosystem. However, at the same time, the management of these data is often outsourced to the private sector,positing risks of overreliance on the private sector.

This is often referred to as commercial lock-in or 'vendor lock-in', whereby a defence agency becomes overly dependent on a single supplier or contractor for a defence product, resulting in a range of issues from interoperability to monopolisation to price extortion. We shall return to this point in Sect. 3.

To "avoid vendor lock-in and promote optionality" and taking steps to unlock defence data to enable "complex, multi-party, secure data-sharing" ('Defence Artificial Intelligence Strategy' 2022), the MoD has also promised to pursue reforms to the defence acquisition process to enhance open standards[7] and interoperability. For example, in a report to the Parliament, the Secretary of State for Defence articulated the importance of ensuring that industry contracts delivery comply with open standards and can be integrated into the defence 'system of systems' before it enters into service (UK Ministry of Defence 2023).

The US Department of Defense (DoD) has put in place a wide range of initiatives to prompt the sharing of battlefield data to support innovation. These include data lakes and data-brokering solutions (see Appendix). DoD has prioritised using data to enable the Joint All-Domain Command and Control warfighting capabilities,[8] it has also been very forward thinking in attempting to harness data's value for defence technological innovation. Its 2020 Data Strategy proposes steps to make all DoD data visible, accessible, understandable, linked, trustworthy, interoperable, and secure. A series of data decrees released in 2021 provided further impetus to "maximize data-sharing and rights for data use" and treat all DoD data as enterprise resources (Hicks 2021).

Regarding preferences for a data management system, US defence policymakers have favoured a *federated data catalogue* with "automated data interfaces" built with "industry-standard, non-proprietary, preferably open-source, technologies, protocols, and payloads" (Hicks 2021). As the DoD's 2023 AI Adoption Strategy posits, a federated system is best suited to support DoD's mix of centralised and decentralised services ('2023 Data, Analytics, and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage' 2023). A 2024 report by the Defense Innovation Board concurs that a federated data catalogue for defence technology—accessible by a trusted community of industry vendors, war fighters, and acquisition programme executives—is needed to integrate data sources from multiple vendors across the defence industrial base (Defense Innovation Board 2024). We shall return to federated solutions for data-sharing in Sect. 5 and in the Appendix.

The efficacy of the DoD approach is undermined by government's insufficient property rights over data collected via technology platforms developed by industry. For example, a 2024 report by the US Defense Innovation Board notes that DoD is often unable to access and manage data originating from systems it subscribes to or builds in collaboration with industry, partly because of uneven requirements for vendors to provide their application programming interfaces (Defense Innovation Board 2024). DoD's fragmented data access rights undermine its ability to aggregate and ensemble from various platforms and services for future use. Hence, it was recommended that DoD secure contractual data access to ensure it can leverage these resources for future data transformations and ensembles (Defense Innovation Board 2024).

These constraints offer an important lesson when considering policies strategies to control and leverage battlefield data (more broadly defence data): without a substantial reframing of the role of the DOD in data management, and without a comprehensive approach to procurement and a redefined relationship between private and public actors in defence, the DoD's 2023 AI Adoption Strategy risks remaining experimental rather than an opportunity to transform data management in defence.

NATO has also developed strategies focussing on defence data. Although its main focus remains data standardization and real-time information sharing amongst its members. To aid NATO's increasing need for interoperability, NATO launched the Alliance Data Sharing Ecosystem pilot initiative in 2024 to foster secure data-sharing at speed and scale to enhance situational awareness and data-driven decision-making.[9] It aims to connect data from both external stakeholders (e.g. academia and industry) and internal ones (e.g. Digital Ocean, Alliance Future Surveillance and Control) through a federation model for data exchange.[10]It remains to be seen whether and how data interoperability is for NATO a goal in itself or a preliminary step to foster the sharing and use of defence data to aid the develop AI, and other digital, defence capabilities.

[7] These are publicly available specifications and protocols that enable interoperability between different AI systems, models, and platforms without proprietary restrictions.

[8] https://www.defense.gov/News/News-Stories/Article/Article/3683482/hicks-announces-delivery-of-initial-cjadc2-capability/.

[9] https://www.nato.int/cps/fr/natohq/news_229523.htm?selectedLocale=en.

[10] https://www.nato.int/nato_static_fl2014/assets/pdf/2024/12/pdf/241213-DBRA.pdf.

Fig. 1 A conceptual map of the challenges related to the management of battlefield data presented in this section

3 Challenges in controlling and managing battlefield data

Curating battlefield data poses severe ethical, legal and social challenges, which vary with the actor in charge of the curation. These include the risks of excessive privatisation of the data and AI capabilities; the loss of digital skills in defence organisations; the erosion of data sovereignty; the infringement of intellectual property (IP) rights; risks of privacy violations and mass surveillance; and the fragmentation of data archives (see Fig. 1). In the subsequent sections, we disentangle these challenges for analytical clarity, though they remain deeply interwoven in practice. For instance, the privatization of data directly impacts data archiving and sovereignty, whilst threats to data sovereignty amplify risks related to privacy breaches and mass surveillance.

These challenges are not limited to battlefield data; rather, they beset the wider transition towards a data-centric paradigm in defence technology innovation, as the defence sector as a whole becomes increasingly digitalised. Thus, insights gained from considering and tackling these challenges specifically with respect to battlefield data could yield valuable lessons to inform broader data policies strategies across the defence sector.

3.1 Privatisation of data, loss of digital skills and capabilities

Private technology companies and defence start-ups have become crucial players in the provision of defence capabilities. Big Tech provides the fundamental digital infrastructure (e.g. cloud servers, satellite services) to enable digital warfighting. In Ukraine, for example, Microsoft provided the cybersecurity capabilities to thwart Russia's attacks on Ukraine's critical infrastructure, Amazon helped migrate critical Ukrainian government data out of the country to prevent data loss from physical destruction of hardware and servers, and SpaceX formed the backbone of Ukraine's military communications via its Starlink satellites (Franke 2024). Big Tech are not the only new entrants to the defence industry. According to a 2024 report by McKinsey, defence start-ups are well-positioned to provide a range of novel capabilities—including sensing and connectivity; advanced computing and software; autonomous systems; and biotechnology (Klempner et al. 2024).

Private companies often pioneer technologies later adopted by government organizations, fostering a symbiotic relationship between the two sectors (Sezal and Giumelli 2022). Yet, the growing dependence on private companies to collect, manage, analyse, and disseminate battlefield data intensifies the ongoing transfer of digital skills and resources from the public to the private sector. Indeed, this continual

transfer of expertise and resources risks undermining the capacity of defence organizations to control and govern digital technologies, including battlefield data, independently. This heightens the risk that accountability and responsibility gaps may occur (Gregory et al. 2021); as private entities operate under commercial interests rather than public accountability frameworks, making it challenging to enforce transparency, oversight, and adherence to ethical standards. Additionally, if these companies face financial difficulties, policy changes, or external pressures, this could create severe vulnerabilities to defence organisations. For example, if a key supplier of critical defence components goes bankrupt or faces regulatory restrictions, it could disrupt military supply chains and compromise national security.

If the transfer of resources and capabilities continues, the relationship between the public and private sectors in defence may increasingly resemble a form of data feudalism. The idea describes the impact of private companies' outsized control over data and other digital assets on societal structures, including public institutions (Saura García 2024), resulting in large power asymmetries between tech companies and the different actors in modern societies. Applied to the case of defence organisations, data feudalism increases the risks that these organisations may find themselves overly dependent and even exploited by tech providers, should they fail to assert control over battlefield data. This is not a remote risk. For example, the UK MoD observes that,

> "[a] large amount of defence data is held by suppliers and third parties, making it difficult to access, update without cost or leverage for exploitation" (UK Ministry of Defence 2021).

Commercial lock-in of data aggravates the risks of data feudalism. The case of Ukraine offers a good example. This country has witnessed an influx of private defence technology companies to support its defence against Russia's full scale invasion in February 2022 (Soesanto 2024). Without data standardisation and the government's assertion of data rights, the proliferation of actors collecting battlefield data will only create more data siloes that remain inaccessible to national defence organisation to develop and improve defence technologies. At the same time, over dependence from private companies for defence data may erode national decision-making capacity, compromising strategic autonomy. In this sense, questions concerning the privatisation of data are also a matter of national sovereignty, as we shall see in the next section.

3.2 Data sovereignty erosion

Scholars generally agree that the global reach of tech providers can complicate traditional notions of state control and authority (Gu 2024). The term "technopolarity" is quite relevant here to describe "an emerging world order in which the largest technology companies rival nation-states as the primary players in international affairs".[11] Private firms, through their control of critical data, technologies, and skills may seek to shape, or influence national defence policies and strategies in ways that align with their corporate interests rather than national security priorities (Khanal et al. 2024). Technology companies may also act in ways that defy the national security objectives of sovereign states. This was the case for example with Starlink's refusal to turn on its satellite communications in support for an Ukrainian offensive in September 2023 (Borger 2023). Risks for data sovereignty also occur when foreign actors collect and use battlefield data without granting the local government adequate control over data flow, thereby undermining national authority over critical data. This type of risk became evident, for example, when reports found that private companies collected and sold location data, enabling the tracking of US military and intelligence personnel, allowing foreign entities to monitor their movements without the US government's consent, thereby undermining data sovereignty.[12]

The increasing prominence of dual-use technology companies—like Google, Amazon, Microsoft, SpaceX and smaller defence start-ups—also challenges to data sovereignty and governance. This is because these companies have different incentives than traditional defence contractors. Unlike traditional defence contractors, which rely heavily on public demand for growth and profits, these companies often derive the majority of their profits from the civilian market, granting them greater bargaining power vis-à-vis public sector procurers and amplifying the risk of regulatory capture (Coveri et al. 2024).

As defence organisations deepen their collaboration with tech companies, it is imperative to shape these partnerships to prevent private entities in defence from prioritising corporate interests over the public good when the two are in conflict. Ensuring alignment between technological innovation and national defence objectives remains a critical challenge in preserving public accountability and strategic autonomy.

3.3 IP and innovation conflicts

The transferring of control of battlefield data from tech firms to defence organisations also poses commercial challenges. For example, it could introduce significant risks for intellectual property (IP). Defence contractors invest heavily in

[11] Bremmer, Ian. 2021. 'How Big Tech Will Reshape the Global Order'. *Foreign Affairs*, October. https://www.foreignaffairs.com/articles/world/ian-bremmer-big-tech-global-order.

[12] https://www.wired.com/story/phone-data-us-soldiers-spies-nuclear-germany/.

developing proprietary AI models, data analytics frameworks, and AI systems. These assets represent substantial intellectual property holdings, which are at risk when shared with government entities. When governments demand access to such proprietary datasets, private firms risk losing their competitive advantage, as defence organisations might replicate, adapt, or share proprietary technologies with competitors without adequate compensation. Indeed, government-imposed data-sharing may disincentivise the private sector investment in research and development fearing that innovations will be expropriated without sufficient safeguards.[13]

Additionally, corporate confidentiality agreements protect proprietary data from unauthorised disclosure. Government contracts are subject to the same stipulations. For example, under the relevant US laws, the scope of the government's right to use, release, or disclose the technical data underlying an item typically depends on who paid for its development (Baker et al. 2015). Only in cases where a defence product is developed exclusively through federal funding, then the government has unlimited data rights. When private funding is involved, the government's data rights can be much more restricted (Peters 2022).

Should governments attempt to mandate access to privately held information, legal disputes may arise over jurisdictional control, ownership rights, and the extent to which governments can demand corporate trade secrets (Morten 2023; Levine and Sarnoff 2024). Some companies fear that excessive government oversight and intervention could lead to forced technology transfers, a common concern in government procurement and supplier agreements in international trade disputes. Addressing these issues adequately is crucial to the development of a digitalised, data-centric defence. As the reader may recall from Sect. 2, IP protection is the main obstacle to the successful implementation of US defence data strategy.

To mitigate risks of over reliance from the private sector and erosion of data sovereignty, a paradigm shift is needed to reposition defence organisations as central actors in controlling battlefield data whilst curbing the privatisation of data and digital skills. To be successful, this shift must envisage robust incentives for the private sector to continue fostering innovation, ensuring that national security imperatives coexist with the vitality of technological innovation (Taddeo, Blanchard, and Pundyk 2024).

3.4 Excessive data collection

The collection of battlefield data often involves sensitive personal data concerning military personnel, non-combatants, and enemy combatants. Excessive data collection—disproportionate and unnecessary—as well as any unauthorised access to such data, whether through cyberattacks, insider threats, or inadequate security protocols, may lead to the exposure of critical intelligence, subsequently placing individuals and their privacy at risks. For example, biometric data, such as facial recognition profiles, fingerprints, and DNA samples, are increasingly utilised in conflict zones (Jacobsen 2022). These are highly sensitive data and their collection and storage pose risks for human rights as wells as for national security.[14]

The digitalisation of defence may prompt excessive data collection and undue surveillance. Consider, for example, 'data creep'. This occurs when the ability to analyse data expands, notably through advancements in AI, resulting in an escalation of data collection practices (United Nations High Commissioner for Human Rights 2021, 4). Here, the intrinsic characteristics of AI serve as the driving force behind the acquisition of increasing volumes of data, encompassing diverse types and sources. Consequently, defence organisations and contractors may engage in extensive, disproportionate data collection; when this includes personal data, privacy is at risks (Taddeo 2013).

Should governments use these data for national security purposes, this may also lead to undue surveillance. This is a risk that is already evident when considering data collection for the use of AI for intelligence purposes (Blanchard and Taddeo 2023). For example, Weinbaum and Shanahan show that,

> Current intelligence practices involve extracting information of value from large datasets of cross discipline (cross-intelligence) information – the needle in the haystack – leading to the bulk collection and storage of hay in hopes that eventually all needles will exist inside. In a more data-orientated era, it is increasingly possible to draw intelligence of value from the data in aggregate (temporal and geospatial behaviour patterns,

[13] Tech companies navigate complex legal frameworks when considering whether to share their data with government institutions. Regulations, such as the General Data Protection Regulation (GDPR) in Europe and the California Consumer Privacy Act (CCPA) in the US, impose stringent requirements on how data can be collected, processed, and shared. But these frameworks often clash with governmental demands for access to private sector datasets, particularly in areas involving national defence and security exposing them to further liabilities.

[14] Note that whilst the obligations and rights provided by regulations like the EU's GDPR may be restricted to safeguard national security, defence, and public security, such restrictions remain conditional to the respect fundamental rights and freedoms and need to pass a test of necessity and proportionality on a case-by-case basis. They are not blanket carve-outs for national security and defence applications (Afina and Grand-Clément 2024).

> for example). This can result in an ironic dilemma in which there is too much data for humans to search effectively for needles, yet not enough accessible data from which to draw and validate useful intelligence. (Weinbaum and Shanahan 2018, 6)

At the same time, should foreign private companies controlling battlefield data decide to grant access to their domestic government, on top of eroding national data sovereignty, this would also lead to breaching privacy, and subjecting foreign citizens to undue surveillance. Hence, it is important to establish clear regulations regarding the scope and purpose of battlefield data collection, the authorised entities to access them, oversight mechanisms to ensure compliance with such regulations, and criteria to ensure necessary and proportionate data collection and access.

3.5 Fragmentation of data archives

Defence organisations and private contractors often operate within siloed data environments, this hinders seamless data integration. Problems like lack of common data formats, standards, and protocols are amplified at the alliance level, as more national defence organisations have developed distinctive practices over time. Various initiatives—for example, NATO's Data Exploitation Framework Policy and the Data Exploitation Programme—have attempted to increase interconnectivity across the allies' different data environments, but efforts to create an integrated and singular secure data environment across alliances remain inchoate (Soare 2023; NATO 2024).

Acquisition strategy is another source of the problem. Until recently, the application-centric approach had been the paradigm for defence acquisition in the US. One expert noted that DoD's focus on

> buying next-generation platforms rather than the sensors, payloads, and communications systems needed to make both existing and next-generation platforms work together more effectively is a deep cultural limitation of the military. (Harrison 2021)

This is the root cause of many interoperability limitations present in DoD today, which is why the Department is increasingly prioritising modular systems with substitutable components in its procurement strategy using the Modular Open Systems Approach.[15] A similar approach has been developed by DoD's Chief Digital And Artificial Intelligence Office, which launched the Open Data and Applications Government-owned Interoperable Repositories initiative in 2024 to create a "multi-vendor ecosystem" for industry and government to integrate platforms and tools whilst preserving government data ownership and industry IP.[16]

Applications- or platforms-centric data practices create another challenge: data are siloed within disparate defence branches. Because data practices are tailored to the needs of specific defence applications, there is a lack of common standards in formatting and structuring the data across defence. For instance, developed by the US Airforce and the Army respectively, both F-35 s and land power assets have stovepiped communications and sensory networks, meaning that the Army's platforms cannot share information effectively with the Air Force's (Chakraborty 2021; McGiffin 2024). This is why, intermediary nodes and communications networks are necessary to put the platforms in contact, reducing the readiness of data-sharing across different platforms (Hoehn 2022, 18). Adding to the interoperability challenge is the fact that each component of the defence department has developed an idiosyncratic lexicon for its data.

Data sharing across classification levels is another persistent challenge. It emerges when considering the tension between data-sharing and 'need to know' principle, which implies that a case has to be made to access highly sensitive data, adding an extra layer of bureaucracy to the process. For example, the US national security community has long acknowledged overclassification as a significant barrier to efficient data exchange (Cuillier 2023). The isolation of classified IT systems, driven by stringent security requirements has led to a proliferation of incompatible data environments. The MOD exemplifies this issue, admitting in March 2024 that it maintains "too many secret cloud capabilities" and aims to transition to a single secret cloud provider to streamline access to classified data (McClintock et al. 2024).

Due to the absence of cloud connectivity, classified data often must be stored or transmitted manually, creating substantial logistical challenges and further complicating inter-organisational data-sharing. The decision-making process for releasing classified data is equally cumbersome, frequently involving lengthy reviews by multiple stakeholders. For instance, components of the DOD often require case-by-case authorisation from foreign disclosure officers and data owners before sharing relevant information with allies and mission partners. These bureaucratic processes, coupled with fragmented technological architectures, impede timely and effective collaboration, raising questions about

[15] https://uscode.house.gov/view.xhtml?req=(title:10%20section:4401%20edition:prelim)%20OR%20(granuleid:USC-prelim-title10-section4401)&f=treesort&edition=prelim&num=0&jumpTo=true.

[16] https://www.defense.gov/News/Releases/Release/Article/3791829/cdao-announces-new-approach-to-scaling-data-analytics-and-ai-capabilities/https%3A%2F%2Fwww.defense.gov%2FNews%2FReleases%2FRelease%2FArticle%2F3791829%2Fcdao-announces-new-approach-to-scaling-data-analytics-and-ai-capabilities%2F.

the balance between national security imperatives and operational efficiency.

Lack of consistency in data management can degrade the performance of technologies, particularly AI systems that rely on such data for training and operational effectiveness. Thus, overcoming this fragmentation is a goal, but it is also a requirement for data-centric defence. Defence organisations leading the collection and management of battlefield data would pursue consistent practices. At the same time, however, the definition of shared standards for data management and curation is as a preliminary step for defence organisations if these are to control and curate battlefield data and leverage their potential to develop AI capabilities.

The analysis proposed in this section reveals that the transition to a data-centric defence creates a tension between technological capability and governance control. The growing dependence on private technology companies for battlefield data collection risks data feudalism, where defence organisations lose strategic autonomy to commercial interests, whilst fragmented data systems across incompatible platforms and classification levels undermine the interoperability that data-centric approaches promise to deliver. Combined with eroding public sector digital capabilities, complex intellectual property disputes, and inadequate privacy safeguards, these challenges suggest that implementing data-centric defence successfully requires defence organisations to reassert control over battlefield data whilst establishing robust frameworks that balance innovation incentives with sovereignty protection and ethical governance. In the rest of this article, we outline an approach to meet these needs.

4 Battlefield data as an artificial club good

The gaps and challenges outlined in Sects. 2 and 3 can be tackled effectively through a governance approach that balances ethics, i.e. respecting individual rights and the values of liberal democracies, Just War Theory principles, and AI ethics principles; robust and effective AI defence capabilities; and digital sovereignty. In this article, we argue that this balance is best achieved once we understand the economic nature of battlefield data and the ethical obligations of defence organisations.

Battlefield data are relatively non-rivalrous. Like other types of digital data, they are not consumed by access/use. Yet, their strategic value diminishes if these data are accessed by all interested actors, especially adversaries. They are also non-excludable.[17] In principle, anyone on the battlefield may record data about the environment and the activities within it. For example, a soldier (or a non-combatant who has access to a battlefield) can record data about weather patterns, drone activity, and destroyed tanks. In economic terms, by nature, battlefield data are an impure public good. Yet, national defence and security imperatives demand access restrictions, turning these data into an *artificial club good*—non-rivalrous and selectively accessible. This explains why, thus far, the private-led curation of battlefield data has faced little resistance. However, this approach has proved to be problematic. It is at the root of most of the challenges we described in Sect. 3 and, going forward, risks hindering the responsible development and deployment of AI in defence and to undermine the autonomy of defence organisations and their control over AI technologies. This is why we argue that we should shift from a private-led to a public-led approach to the management of these data.

Defence organisations should act as *club manager*[18] for this artificial club good to safeguard data and leverage their value. As club manager, defence organisations would be responsible for determining who can access the data, establishing rules for data-sharing and use, maintaining data quality and security, and ensuring that access restrictions serve the strategic interests of the managing organisation whilst maximizing the value derived from the shared resource. Both pragmatic and ethical reasons support this shift. Pragmatically, battlefield data derive from adversarial activities subsidised by the State and concern technologies procured with public funds. These data have huge relevance for national defence and security, so national defence organisations should be in charge of their management. Ethically, defence organisations have obligations concerning AI technologies, which derive from the ethical principles of Just War Theory and those specified for AI in defence—like those adopted by the US, the UK, and NATO (Taddeo et al. 2021, Taddeo 2024) .

Just War Theory provides the foundational framework for establishing the duties of defence organisations to oversee battlefield data governance. These duties stem from core principles that demand strict control over instruments of warfare, including distinction between combatants and civilians, military necessity, and proportionality in response ((Blanchard and Taddeo 2022b; 2022a)). To limit the risks of breaching these ethical principles when using AI in war waging, defence organisations must maintain comprehensive oversight of the technologies they deploy. A defence-led management of battlefield data serve this goal and would

[17] Even if one may imagine that some data—e.g. data about activities inside the cockpit of an F-35—may not be easily accessible. We still take battlefield data to be non-excludable as in great part these data concern dynamics and events observable at least by those present on the battlefield.

[18] A club manager is organization or entity that controls access to and oversees the distribution of a club good.

create pathways for developing more robust and reliable AI systems.

In the same way, acting as club managers of battlefield data would enable defence organisation to discharge obligations posed by the AI ethics principles for defence. Consider for example, 'AI robustness', this is an ethical principle adopted by the US (DIB 2020), UK ('Defence Artificial Intelligence Strategy' 2022), and NATO[19] (Taddeo et al. 2021). Robustness is crucial as a robust AI model is less vulnerable to cyberattacks, third party manipulations, and its outcome is also more predictable, thus it is more reliable and more controllable (Taddeo, McCutcheon, and Floridi 2019). As we mentioned in the introduction, operationally relevant battlefield data are crucial to improve AI robustness (Taddeo et al. 2022). It follows that defence organisations who commit to robustness as an ethics principle informing the AI lifecycle also commit to leverage these data for the development of AI. Robustness is best achieved when developers can rely on big data sets, thus, to be effective battlefield data need to be curated at scale, a task that defence organisations are best placed to achieve.

AI robustness would also be improved if battlefield data were made equally available to all relevant defence contractors procuring AI technologies and their use made mandatory for testing, evaluating, and validating AI technologies before adoption. This task that requires mandatory power, coordination and oversight over diverse set of battlefield data, defence organisations have the authority, power, and reach to act as the necessary institutional bridge between operational requirements, technological capabilities, and ethical obligations, whilst enforcing standardised governance frameworks across all relevant stakeholders and ensuring that battlefield data management serves national defence interests.

Managing these processes would enable defence organisations to participate in the development of technological innovation rather than merely procure and consume it, reducing the risks of over dependence from private actors, of lock-in, and data feudalism. It would also enable them to maintain control of data and their flow, hence mitigating risks to data sovereignty and ensuring that criteria for data collection and assess respect defence needs as well as fundamental rights.

A defence-led management of battlefield data will ensure that their value remains available across the sector to maximise opportunities for innovation. By granting access to all relevant defence contractors and making mandatory testing and evaluation framework based on these data, defence organisations would also mitigate the challenges to IP and innovation described earlier. This is because national defence organisations would shoulder the costs of data collection and curation, thereby subsidising the developing and testing of new technologies. This along with the development of better products and services should incentivise, rather than discourage, the defence technology industry. At the same time, by making these data accessible across the board of contractors, defence organisations would distribute an advantage fairly. A shared pool of high-quality, high-value data will lift all boats, effectively supporting national (like-minded countries) defence industries and overall technological innovation.

It should also be noted that although defence organisations' assertion of data rights would diminish defence contractors' claims to IP over battlefield data, this approach would spur innovation by aiding defence tech start-ups; leading in the medium-term to a more competitive and active industrial sector. In the absence of robust data-sharing policies, these start-ups struggle to compete with established vendors as they lack access to the extensive battlefield data crucial for digital defence innovations. A defence-led, governance structure for data management has also the potential to remedy the fragmentation of digital archives. As defence organisations centralise control over battlefield data, they have greater visibility over where data siloes occur and greater authority in bridging and connecting these pockets of data (more on this in Sect. 5).

One may claim that this approach is not feasible both in terms of the costs (both human and economic resources are needed) that defence organisations should bear and in terms of reactions of the private sector. In the short run, this approach would incur substantial costs for defence organisations, but such costs are outweighed by the medium-term anticipated benefits—ranging from enhanced control over data, increased robustness of defence AI systems, and the optimisation of AI capabilities, ethically sound development of AI, to the broader promotion of technological innovation. With respect to the reaction of the private sector, it is worth recalling the findings of our policy review. As the reader may recall, the DoD has already started envisioning, designing, and implementing measures that head in the same direction of the approach proposed here. However, these measures remain a partial success due to the lack of a systemic approach, that would link battlefield data collection with shared access to these data to support AI innovation, thus offering incentives to the private sector to balance for the erosion of IP rights. It is the acquisition of data without returning any clear advantage for the private sector that limits its current US approach to battlefield data. Leveraging the potential of these data for AI innovation as part of a defence-led management would create a virtuous cycle where private innovation serves public interests and public investment enables private advancement, reducing friction with technology

[19] https://www.nato.int/docu/review/articles/2021/10/25/an-artificial-intelligence-strategy-for-nato/index.html.

providers whilst enhancing control and autonomy of defence organisations. The approach proposed here frames a public-led management of battlefield data in a wider framework tailored to the need of an ever-more digitalised defence. Here, we agree with Keynes that

> the important thing for government is not to do things which individuals are doing already, and to do them a little better or a little worse; but to do those things which at present are not done at all. (Keynes 2010)

We hold this to be true for battlefield data and defence organizations as well. A public-led approach to battlefield data curation is not merely an enhancement of existing practices but a fundamental shift—one that ensures data are managed at scale, not merely for profit, but as an ethical obligation develop responsible defence technologies. This transformation demands systemic changes in procurement, public–private relations, digital infrastructure, and operational processes. Such a shift carries substantial costs, requires coordinated effort, and necessitates a medium-term strategy rooted in the respect of the values of liberal democracies and the principles of Just War Theory. This is why this shift is one of things "not done at all" by the private sector and which falls under State's responsibility, particularly of its defence organizations.

The opposite solution, continuing delegating the stewardship of battlefield data to private actors, would be operationally and ethically problematic as it would exacerbate the challenges described in Sect. 3. These challenges—from data feudalism to sovereignty erosion—are not isolated failures but symptoms of a paradigm that prioritizes profit over strategic autonomy and ethical governance. Continuing with this approach would also lead severe opportunity cost in terms of development of technological innovation and hinder the responsible development and use of AI in defence. If properly designed as defence-led management of battlefield, data could overcome these limitations and foster responsible AI in defence. In the next section, we offer two sets of policy recommendation to inform the design of such a governance approach.

5 Recommendations

The challenges outlined above can be tackled effectively through governance that balances ethics, AI robustness, and digital sovereignty. Here, we offer two sets of recommendations that rest on these three elements to support both procedural and technical choices that defence organisations should consider in acting as club manager for battlefield data. We should note that the recommendations presented in this section result from an approach tailored to emerging governance challenges where comprehensive empirical data remain classified or otherwise unavailable to academic researchers. They result from our policy review of Western defence organisations (Sect. 2), technical feasibility assessments based on existing data management solutions documented in both civilian and declassified military contexts (see Appendix), and the application of established ethical frameworks drawing upon Just War Theory principles. Our risk mitigation strategies directly address the challenges identified in Sect. 3, creating a coherent link between documented problems and proposed solutions. The recommendations are organised into two complementary categories: procedural measures for internal governance structures and technical approaches for data architecture and management.

5.1 Shaping internal processes to manage battlefield data

We suggest that defence organisations should have:

- Clear boundaries and membership—Defence organisations must define who gets access (e.g. government agencies, allies, vetted contractors) and under what conditions.
- Rules tailored to operational needs—Data policies should reflect battlefield realities, distinguishing between high-security tactical data (real-time data collected during active military operations) and broader strategic information (aggregate, long-term data used for planning, training, and developing AI models, and enhancing defence capabilities). These two categories of data have varying degrees of sensitivity and purpose, and the level of protection and sharing should be adjusted accordingly.
- Set standards for data curation—Defence organisations should establish clear protocols for the secure storage, cataloguing, and maintenance of data to ensure consistency, reliability, and accessibility. This includes specifying formats, metadata requirements, and access controls to facilitate interoperability between systems and enhance the efficiency of data retrieval and utilisation. Effective curation practices should also encompass data quality assurance, regular audits, and the implementation of retention and disposal policies aligned with operational and legal requirements. This measure would help reducing the risks of fragmentation and limited interoperability described in Sect. 3.
- Monitoring and enforcement—Defence organisations should devise measures to assure technical oversight to track data access and prevent misuse, with clear penalties for breaches. This would be particularly relevant to mitigate risks for digital sovereignty.
- Oversight mechanism for responsible practices—Defence organisations should identify and support (for example

ensuring traceability and transparency) a body responsible for monitoring battlefield data collection and management practices to assure that these comply with relevant ethical principles and human rights (see Sect. 3).
- Dispute resolution mechanisms—Conflicts over IP rights, access conditions, and vendor lock-in should be handled through transparent arbitration, avoiding bottlenecks in critical defence operations.

5.2 Technical choices to manage battlefield data

From a technical point of view, the ideal solution needs to ensure the scale, quality, and security of battlefield data. Scalability is necessary for handling and extracting value from an ever-growing volume of data emerging from the contemporary battlefield. But scaling data without safeguarding data quality would create severe ethical risks, degrading the value, useability, and trustworthiness of data for advanced analytics, AI applications, and other defence innovations (more on this in the Appendix). Security is a key requirement as polluted data may lead to harmful behaviour by AI systems, limited control of these systems and the risk of noncompliance with international humanitarian laws, and severe risks for the safety and security of military personnel.

We suggest that a state-led data collection and management should not translate into centralised solutions for data collection, storage, and curation, e.g. data lakes and data warehouses (see Appendix). Instead, defence organisations should prefer distributed approaches and in particular develop a *federated model for data management*. One form of federated data management is data mesh, which shifts from traditional centralised data management to a domain-oriented model approach. This approach is being tested by the US DoD at the moment (see Sect. 2) and best balances efficiency with security. Data ownership is distributed across individual domains, where teams manage their own data as a product. Domain teams are entrusted with autonomy and domain-local decision-making power but adhere to a set of global rules informed by global specializations, such as interoperability, documentation, security, privacy, and compliance policies (CDAO 2024).

This approach is ideal for managing data in high-risk domains, like defence, as domain ownership offers the advantage of scale by removing common bottlenecks associated with centralised systems. In data lake or data warehousing architectures, centralised data teams are responsible for ensuring the quality and integrity of data. By contrast, domain ownership ascribes responsibility of curation to closer to the source of the data. Rather than aim to port data into one large, centralised storage, data mesh focuses on *connecting data* wherever they reside using knowledge graphs and data catalogues, streamlining the process by which data become usable products and yield actionable insights and overcoming the fragmentation of digital archives (Dehghani 2022).

Reduced dependencies on central data management lead to higher scalability, allowing the organization to scale horizontally (i.e. more data sources) and vertically (i.e. more consumers) without creating a bottleneck. Data mesh can be effectively complemented with edge computing—bringing computation and data storage closer to data sources (e.g. battlefield sensors)—to enhance also agility (see Appendix). The double-layer of control (central and local) fosters security as it enables multiple points of control whilst also limiting access to data to specific 'regions'. Data included in a data mesh require curation, which foster data quality, limiting the risks for unwanted biases, inconsistencies amongst data, and discourages a 'harvest now, analyse later' approach and related risks for privacy breaches and mass surveillance.

In short, the adopted federated model should balance centralised oversight with domain-level autonomy, by implementing a governance structure that enforces data standards across the organisation, whilst allowing domain teams the flexibility to manage their own data. To ensure standardised governance, defence organisations should

- Create a federated governance team comprising the relevant experts and stakeholders—To define baseline policies on security, compliance, and interoperability whilst delegating operational decision-making to domain teams. Organisations should establish cross-domain governance forums where representatives from each domain collaborate to align their practices with global standards, resolve conflicts, and promote knowledge sharing. This would improve cross-domain coordination whilst retaining the agility of domain ownership.
- Mandate transparency and compliance mechanisms—To ensure equitable and secure data practices, organisations must enforce transparent data access policies across domains. This includes regular audits, reporting mechanisms, and adherence to standardised metadata practices to facilitate interoperability.
- Standardise data curation practices—To prevent inconsistencies in data access policies and regulatory compliance, organisations should define and enforce common data governance protocols. This includes creating shared taxonomies, metadata schemas, and interoperability guidelines that domain teams must adopt.
- Leverage automation and monitoring for policy enforcement—Automated tools should be utilised to monitor compliance with governance policies, detect anomalies, and enforce security measures. This includes AI-driven compliance checks, access control monitoring, and automated reporting on data usage patterns.

The standardised, governance structure should be complemented with measures to empower domain teams to create high-quality data products. To maximise the use of domain-level expertise, defence organisations should

- Establish domain-level authority for data accuracy—A data mesh, particularly when combined with edge computing, should adopt a domain-centric approach to adjudicate the veracity of different data sources. Policies should ensure that data published by each domain are recognised as the authoritative source of truth within their respective areas. This will establish clear lines of accountability and improve trust in data integrity.
- Ensure data fidelity through domain ownership—Since domain ownership places the responsibility for data curation closer to the source, organisations can improve confidence in the fidelity of data products. Policies should require domain teams to implement rigorous data validation mechanisms to prevent distortions and ensure data accuracy from point of capture to consumption. Active metadata—the use of AI/ML-enabled automated tools to record metadata—will be key to generating data lineage information at speed and scale to ensure the fidelity of battlefield data.
- Decentralise data storage to strengthen security—To mitigate security risks, organisations should promote decentralised data storage and access within a data mesh. Distributing data across multiple domains will reduce the risk of large-scale breaches, enhance resilience, and limit the impact of potential cyber threats.

6 Conclusion

Our analysis has showed that current approaches to battlefield data management create systematic vulnerabilities that undermine both operational effectiveness and democratic values. In particular, the dominance of the private sector dominance over battlefield data collection and curation makes defence organisations structurally dependent on commercial entities operating under different incentive structures. This dependency manifests across multiple dimensions: technical lock-in, erosion of institutional capabilities, and compromised data sovereignty.

Our proposed framework reconceptualises battlefield data as an artificial club good, requiring defence organisations to assume the role of club manager. This approach addresses the identified challenges through three mechanisms: redistributing control over strategic assets, establishing equitable access protocols, and creating incentive structures that align private innovation with public objectives. We hope that, as governments increasingly rely on AI across policy domains, the governance frameworks developed for battlefield data may as well be a lesson to inform the governance of AI in other high-risk domains. In these domains, governance is not an add-on, redundant with respect to markets' presumed capable of self-regulation, but an essential mechanism for both risk mitigation and resource optimization. Appropriate governance of AI innovation of high-risk domain is a key ethical obligation for national and supranational organizations charged with their oversight.

Appendix: Data management solutions

Technical solutions for the collection, storing, and accessing of data are either centralised, e.g. data warehouse and data lake, or distributed, e.g. data fabric and data mesh. In this section, we outline these solutions and assess their ethical implications and desirability to support the collection and sharing of battlefield data for developing AI defence capabilities. The data management solutions surveyed below are attempts to achieve some form of scale-quality-security balance. For example, *data warehouses* prioritise quality but trade off scalability. A data warehouse is a centralised repository for storing, integrating, and analysing structured data from multiple sources. It has a schema-on-write approach (Serra 2024). Thus, data stored in a data warehouse undergo a transformation, typically through Extract, Transform, and Load (ETL), to extract data from source systems, enforce data type and data validity standards, and ensure it conforms to the requirements of the data warehouse (Kimball and Caserta 2004).

The ETL process provides a recurring point of intervention to enforce robust governance mechanisms so that data are safe and compliant with regulatory regimes ('Data Mesh vs Data Fabric, Data Lake & Data Warehouse' 2025). For example, defence data engineers could redact battlefield data that may reveal a covert method of intelligence gathering during the ETL process, reducing the impact of potential cyberattacks. Despite its advantage in data quality and security, a data warehouse sacrifices scalability, as it is costly to set up and maintain and the requirement of a defined, structured schema does not work well with unstructured data, which characterise the majority of battlefield data.

Data lakes offer a centralised alternative to data warehouse. These are a highly scalable and flexible storage solution, enabling organizations to ingest, store, and analyse data without the constraints of predefined schemas or the need to perform upfront work (Ahmad and Batan 2023). In contrast with data warehouses' schema-on-write approach, data lakes are schema-on-read (Serra 2024). Thus, this architecture allows organizations to accumulate large quantities of various types of data, including those in raw and unstructured form, favouring scalability. This flexibility and scalability make data lakes suitable for pooling

defence data to inform defence decisions in real time. For example, DELTA, a system developed by Ukraine to facilitate military command and control, has been described as the "largest Ukrainian integration platform and national data lake that operates in the cloud" (Giordano 2024). At the Coalition Warrior Interoperability Exercise (CWIX), NATO's biggest interoperability event, technicians, scientists, operators, and engineers from 35 allied nations and organisations have tested the use of data lakes to make data discoverable, retrievable, and understandable in a coalition environment (Giordano 2022).

Data lakes' ability to stockpile battlefield data also offers advantages in technological innovations in the long term. At the moment of ingestion, analysts are not required to have theories or hypotheses as to which and how data will be relevant. A data lake enables the collection of any data in case they become valuable for future use cases (Serra 2024). However, data lakes' lax data intake may encourage a "harvest now, analyse later" approach: data handlers mindlessly accumulate and retain data just because they can, failing to contend with the associated ethical and legal risks, such as whether the collection of data might require consent from data subjects, how their rights might be safeguarded, and what remedy or accountability mechanisms are in place to uphold their rights. These risks are especially pronounced when data lakes enable the accumulation of large volumes of legacy data without robust deletion or data traceability mechanisms, which makes it difficult for operators to comply with data minimisation, the right for individuals to request the deletion of their data, or the right to be forgotten (Ahmad and Batan 2023).

The accumulation of data in data lakes could also lead to severe security risks. A single, data lake is a one-size-fits-all solution for storing data regardless of the level of security classification. But some incoming data might be more sensitive than others and may require a stricter mechanism to ensure their security (L'Esteve 2023). For instance, the leakage of personal data of combatants could be more damaging than that of data about the battlefield environment because the former could potentially be used by an adversary for personalised attack and targeting. Mixing troves of data of varying degrees of sensitivity would heighten the challenge of isolating and address severe security risks.

Problems also emerge when considering data quality. Data lakes' unselective intake of data could also pose the challenge establishing a single, authoritative "version of truth" (Eberhard Hechler, Weihrauch, and Wu 2023). Different data inputs—whether from drones, satellites, sensors, or human intelligence—may provide conflicting or outdated information regarding the same event, resulting in competing versions of the data that must be reconciled to determine which one is most accurate and reliable. It risks feeding ambiguous or contradictory information, potentially leading to misidentification of targets, inefficient logistics, or even catastrophic friendly fire incidents.

The heterogeneity of data could lead to inconsistent data formats, varying quality standards, and disparate semantic conventions. Without robust governance, data lakes can become *data swamps*, where vast quantities of low-quality or disorganised data are dumped without plans of data enrichment (Ahmad and Batan 2023). This increases the cost of maintenance and storage, obscures analytic insights, and increase regulatory noncompliance risks. Data swamps pose severe ethical risks for as fairness, accountability, transparency, and privacy (Ahmad and Batan 2023). For instance, data lakes are rife with the risk of bias and discrimination when used for data-driven decision-making. They often contain vast amounts of historical data, which may reflect existing biases and inequalities. This can lead to severe problems when considering the developing of AI capabilities, for example systems for target identifications of autonomous weapon systems (Taddeo and Blanchard 2022). In this case, data may convey a bias that could lead to misidentification of non-combatants, undermining compliance with international humanitarian laws. To this end, Afina and Grand-Clément argue that AI targeting systems trained on battlefield data collected in a specific part of the world with different demographic realities could erroneously associate certain ethnicities with combatant status (Afina and Grand-Clément 2024).

When data lakes include data originating from different jurisdictions, interoperability becomes difficult, as it may be challenging to govern data lakes in a way that respect the applicable domestic law constraints of the different members of a coalition. For example, when it comes to data privacy laws, legal diversity within the NATO alliance is wide, consisting of EU members; three additional members implementing the GDPR and the Institutional GDPR; and six countries with their individual non-GDPR data privacy laws (Housen-Couriel 2022). Beyond data privacy and protection, these countries may also have different legal interpretation of aspects of international humanitarian laws—including their legal classification of combatants and non-combatants, rules on detention of combatants and non-combatants, and the rules of engagement (Housen-Couriel 2022). Data generated by coalition members may reflect these differences, which could lead to a hidden bias if data are being shared across the coalition without the proper metadata documentation that detail how certain coding decisions are made.

Data fabric and *data mesh* are distributed approaches to data management. Both have only recently emerged, and there is no clear consensus on how to define them. By way of illustration, a data fabric is

> a design concept that serves as an integrated layer (fabric) of data and connecting processes. A data fabric utilizes continuous analytics over existing, discover-

> able and inferenced metadata assets to support the design, deployment and utilization of integrated and reusable data across all environments, including hybrid and multi-cloud platforms. ('What Is Data Fabric? Uses, Definition & Trends', n.d.)
>
> Its core capability is taking in
>
> metadata from participating systems and users, analyzes it, and produces alerts and recommendations highlighting how data could be better organized, integrated, given meaning and used to improve the user experience and business outcomes. ('What Is Data Fabric? Uses, Definition & Trends', n.d.)

Defence organisations' digital transformation strategies increasingly reference the concept of data fabric. To implement its Digital Transformation Vision, NATO is developing an alliance-wide Digital Backbone to facilitate integration and interoperability across domains and platforms. A "federated data fabric" is a central component of the NATO Digital Backbone (NDBB), providing the technical means for connecting "sensors, decision makers, actors and effectors, across the various organizational, national, operational and security domain boundaries" ('The NATO Digital Backbone Reference Architecture' 2024).

The DOD supports the use of data-sharing options by establishing a federated data fabric for

> sharing information through interfaces and services to discover, understand and exchange data with partners across all domains, echelons and security. (Department of Defense 2022)

Data fabric is understood to be an effective tool for facilitating the secure and rapid flow of data between different compartments of the defence enterprise.

A data fabric can incorporate data lakes or data warehouses—but with added technological features to enable quicker discoverability of data and other governance measures. *Active metadata* are a key element of a data fabric (or automated metadata enrichment[20]). A data fabric centres on *metadata catalogue*—i.e. a repository that stores information about data assets, including their structure, relationships, and characteristics (Serra 2024)—which enhances the ability of the analyst to understand data lineage. There are already being implemented. For example, the US military has taken steps to create DoD Federated Data Catalog to publish metadata of data assets within DoD as required by the DoD Data Decrees published in 2021 (Hicks 2021). This federated approach to data cataloguing enables the exchange of descriptive metadata whilst empowering each DoD component to govern its own data according to its needs (Spirk 2021).

Data mesh departs from centralised solution to a domain-oriented approach: data ownership is distributed across individual domains, where teams manage their own data as a product. This approach rests on four key principles: domain ownership,[21] data as a product, self-serve data platforms, and federated computational governance (Dehghani 2022). Domain ownership entails decentralising the ownership of analytical data to the domain closest to the data source or their main consumers. Each domain is responsible for curating and sharing its data as a product[22] on self-serve data platforms, letting users from other domain teams to discover, trust, and use the data at their convenience. Effective data governance is enabled by a federated governance model consisting of domain data product owners and data platform product owners, who are entrusted with autonomy and domain-local decision-making power but adhere to a set of global rules informed by global specializations, such as interoperability, documentation, security, privacy, and compliance policies (Dehghani 2022; CDAs 2024).

Author contributions The order of the authors reflects the significance of their contribution to the article. MT and BK made substantial contributions to the conception or design of the work; or the acquisition, analysis, or interpretation of data; MT, BK, and JN, drafted the work or revised it critically for important intellectual content; approved the version to be published; MT, BK, JN agree to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Funding This work was supported by the National Institute of Science and Technology (INCT) for Diabetes and Obesity, CNPq, Federal Univesity of Ceara and FUNCAP.

Data availability No datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.MT is a member of the Ethics Advisory Panel on Ethics of AI of the UK Ministry of Defence.

[20] Active metadata is AI/ML-augmented metadata, generated by applying AI/ML techniques to metadata to gain additional actionable insight from metadata, which can be used to further automate Data Fabric and Data Mesh tasks. (Hechler et al. 2023).

[21] Domain ownership is a data management approach where individual business units or operational domains maintain direct responsibility for collecting, curating, and governing their own data as authoritative products, rather than centralising these functions.

[22] Treating data as a product means applying *product thinking* to domain-oriented data. Data must be feasible, valuable, and usable.

References

'2023 Data, Analytics, and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage'. 2023. Department of Defense

Baker JM, McCarthy JE, Haque S, Raddock A (2015) Government data rights challenges: tips on how to avoid & respond. Contract Management. https://www.crowell.com/a/web/f7ZQqG4BKkvnKM2Tbw6Sxo/4TtkH6/11012015-government-data-rights-challenges-tips-on-how-to-avoid-and-respond-baker-haque-mccarthy-raddock.pdf

Blanchard, Alexander, and Mariarosaria Taddeo. 2022a. 'Autonomous Weapon Systems and Jus Ad Bellum'. AI & SOCIETY, ahead of print, March 19. https://doi.org/10.1007/s00146-022-01425-y.

Blanchard, Alexander, and Mariarosaria Taddeo. 2022b. 'Jus in Bello Necessity, The Requirement of Minimal Force, and Autonomous Weapons Systems'. Journal of Military Ethics 21 (3–4): 286–303. https://doi.org/10.1080/15027570.2022.2157952.

Blanchard, Alexander, and Mariarosaria Taddeo. 2023. 'The Ethics of Artificial Intelligence for Intelligence Analysis: A Review of the Key Challenges with Recommendations'. Digital Society 2 (1): 12. https://doi.org/10.1007/s44206-023-00036-4.

Borchert H, Schütz T, Verbovszky J (2024) Master and servant: defense AI in Germany. In: Borchert H, Schütz T, Verbovszky J (eds) The very long game: 25 case studies on the global state of defense AI. Springer Nature Switzerland, Cham, pp 195–216. https://doi.org/10.1007/978-3-031-58649-1_11

Borger J (2023) Elon musk ordered Starlink to be turned off during Ukraine offensive, book says. The Guardian, 7 Sept2023, sec. Technology. https://www.theguardian.com/technology/2023/sep/07/elon-musk-ordered-starlink-turned-off-ukraine-offensive-biography

Chakraborty A (2021) USAF demonstrates in-flight communication between F-35 and F-22 jets. Airforce Technology (blog). 4 May 2021. https://www.airforce-technology.com/news/usaf-in-flight-communication-f-35-f-22-jets/

Chief Digital and Artificial Intelligence Office (CDAO) (2024) Data mesh reference architecture (DMRA). Department of Defense. https://media.defense.gov/2024/Mar/15/2003414274/-1/-1/1/dmra_paper.PDF#page=2.10

Coveri A, Cozza C, Guarascio D (2024) Blurring boundaries: an analysis of the digital platforms-military nexus. Rev Polit Econ: 1–32. https://doi.org/10.1080/09538259.2024.2395832

Cuillier D (2023) Overclassification overkill: The US Government is drowning in a sea of secrets. The Conversation. 2 Mar 2023. http://theconversation.com/overclassification-overkill-the-us-government-is-drowning-in-a-sea-of-secrets-198917

Defence Artificial Intelligence Strategy (2022) GOV.UK. 15 June 2022. https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy/defence-artificial-intelligence-strategy#strengthen-the-uks-defence-and-security-ai-ecosystem

Defense Innovation Board (2024) Building a DOD data economy. Defense Innovation Board. https://innovation.defense.gov/Portals/63/20240118%20DIB%20Data%20Economy%20Study_Approved-compressed.pdf

Department of Defence (2021) Defence data strategy 2021–2023. Australian Government Department of Defence

Department of Defence (2024a) Defence data strategy 2.0—decision advantage in the data age. Australian Government Department of Defence. https://www.defence.gov.au/about/strategic-planning/defence-data-strategy-20-decision-advantage-data-age

Department of Defence (2024b) Joint data networks. Website. Defence. 19 July 2024. https://www.defence.gov.au/defence-activities/projects/joint-data-networks

Department of National Defence and Canadian Armed Forces (2022) DND/CAF data governance framework. Navigation page. 26 July 2022. https://www.canada.ca/en/department-national-defence/corporate/reports-publications/data-governance.html

DIB (2020) AI principles: recommendations on the ethical use of artificial intelligence by the Department of Defense. https://media.defense.gov/2019/Oct/31/2002204458/-1/-1/0/DIB_AI_PRINCIPLES_PRIMARY_DOCUMENT.PDF

Franke U (2024) How companies go to war. Engelsberg ideas (blog). 16 September 2024. https://engelsbergideas.com/essays/how-companies-go-to-war/

Ghioni, Riccardo, Mariarosaria Taddeo, and Luciano Floridi. 2024. 'Open Source Intelligence and AI: A Systematic Review of the GELSI Literature'. AI & SOCIETY 39 (4): 1827–42. https://doi.org/10.1007/s00146-023-01628-x.

Gregory RW, Henfridsson O, Kaganer E, Kyriakou SH (2021) The role of artificial intelligence and data network effects for creating user value. Acad Manage Rev 46(3):534–551. https://doi.org/10.5465/amr.2019.0178

Gu H (2024) Data, big tech, and the new concept of sovereignty. J Chin Polit Sci 29(4):591–612. https://doi.org/10.1007/s11366-023-09855-1

Harrison T (2021) Battle networks and the future force. https://www.csis.org/analysis/battle-networks-and-future-force

Hicks KA (2021) Creating data advantage. Deputy Secretary of Defense. https://media.defense.gov/2021/May/10/2002638551/-1/-1/0/DEPUTY-SECRETARY-OF-DEFENSE-MEMORANDUM.PDF

Hoehn JR (2020) Intelligence, surveillance, and reconnaissance design for great power competition. Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R46389/4#page=33.54

Hoehn JR (2022) Joint all-domain command and control: background and issues for congress. Congressional Research Service

Jacobsen KL (2022) Biometric data flows and unintended consequences of counterterrorism. Int Rev Red Cross. https://doi.org/10.1017/S1816383121000928

Keynes JM (2010) Essays in Persuasion. New ed. Palgrave Macmillan, Basingstoke, New York

Khanal S, Zhang H, Taeihagh A (2024) Why and how is the power of Big Tech increasing in the policy process? The case of generative AI. Policy Soc. https://doi.org/10.1093/polsoc/puae012

Klempner J, Rodriguez C, Swartz D (2024) A rising wave of tech disruptors: the future of defense innovation? McKinsey (blog). 22 Feb 2024. https://www.mckinsey.com/industries/aerospace-and-defense/our-insights/a-rising-wave-of-tech-disruptors-the-future-of-defense-innovation

L'Esteve RC (2023) Designing a secure data lake. In: L'Esteve RC (ed) The cloud leader's handbook. Apress, Berkeley, CA, 183–201. https://doi.org/10.1007/978-1-4842-9526-7_11

Levine DS, Sarnoff JD (2024) Compelling trade secret sharing. In: Sun H, Sunder M (eds) Intellectual property, COVID-19 and the next pandemic, 1st ed. Cambridge University Press, 287–314. https://doi.org/10.1017/9781009282406.015

Little A (2023) New Zealand defence force: information management programme. Office of the Minister of Defence. https://www.nzdf.mil.nz/assets/Uploads/DocumentLibrary/NZDF-Information-Management-Programme.pdf

Martin K, Liversain L (2024) a winding road before scaling-up? Defense AI in France. In: Borchert H, Schütz T, Verbovszky J (eds) The very long game: 25 case studies on the global state of defense AI. Springer Nature Switzerland, Cham, 237–260. https://doi.org/10.1007/978-3-031-58649-1_11

McClintock B, Radin A, Weinbaum C, Pillion SA, Triezenberg BL, Cham J, Elinoff D et al (2024) Allied by design: defining a path to thoughtful allied space power. RAND Corporation. https://www.rand.org/pubs/research_reports/RRA1739-1.html

McGiffin JM (2024) Mission (command) complete: implications of JADC2. Joint Force Q: 113

Meaker M (2023) Everyone wants Ukraine's battlefield data. Wired, 24 July 2023. https://www.wired.com/story/ukraine-government-battlefield-data/

Michel AH (2023) Known unknowns: data issues and military autonomous systems. United Nations Institute for Disarmament Research. https://unidir.org/wp-content/uploads/2023/05/Holland_KnownUnknowns_20210517_0.pdf

Minister of National Defence (2019) Data strategy. The Canadian Department of National Defence and the Canadian Armed Forces. https://www.canada.ca/content/dam/dnd-mdn/documents/reports/data-strategy/2019/dgm-25419-j4j-data-strategy-dia-en.pdf#page=19.09

Morten JC (2023) Publicizing corporate secrets. U. PA. L. REV. https://scholarship.law.columbia.edu/cgi/viewcontent.cgi?params=/context/faculty_scholarship/article/5199/&path_info=Morten_Publicizing_Corporate_Secrets.pdf&utm_source=chatgpt.com

NATO (2024) NATO steps up alliance-wide secure data sharing. NATO, 17 Oct 2024. https://www.nato.int/cps/fr/natohq/news_229523.htm

New Battle Management Software for the Army (2016) Beehive.Govt.Nz. 8 Nov 2016. https://www.beehive.govt.nz/release/new-battle-management-software-army

Peters HM (2022) Intellectual property and technical data in DOD acquisitions. Congressional Research Services. https://crsreports.congress.gov/product/pdf/IF/IF12083

Saura García C (2024) Datafeudalism: the domination of modern societies by Big Tech companies. Philos Technol 37(3):90. https://doi.org/10.1007/s13347-024-00777-1

Sezal MA, Giumelli F (2022) Technology transfer and defence sector dynamics: the case of the Netherlands. Eur Secur 31(4):558–575. https://doi.org/10.1080/09662839.2022.2028277

Soare SR (2023) Digitalisation of defence in NATO and the EU: making European defence fit for the digital age. International Institute for Strategic Studies. https://www.iiss.org/research-paper/2023/08/digitalisation-of-defence--in-nato-and-the-eu/

Soesanto S (2024) The Ukrainian way of digital warfighting: volunteers, applications, and intelligence sharing platforms. Application/pdf. ETH Zurich. https://doi.org/10.3929/ETHZ-B-000685245

Taddeo, Mariarosaria. 2013. 'Cyber Security and Individual Rights, Striking the Right Balance'. Philosophy & Technology 26 (4): 353–56. https://doi.org/10.1007/s13347-013-0140-9.

Taddeo, Mariarosaria. 2024. The Ethics of Artificial Intelligence in Defence. Oxford University Press.

Taddeo, Mariarosaria, Alexander Blanchard, and Kate Pundyk. 2024. 'Consider the Ethical Impacts of Quantum Technologies in Defence — before It's Too Late'. Nature 634 (8035): 779–81. https://doi.org/10.1038/d41586-024-03376-4.

Taddeo, Mariarosaria, Tom McCutcheon, and Luciano Floridi. 2019. 'Trusting Artificial Intelligence in Cybersecurity Is a Double-Edged Sword'. Nature Machine Intelligence 1 (12): 557–60. https://doi.org/10.1038/s42256-019-0109-1.

Taddeo, Mariarosaria, David McNeish, Alexander Blanchard, and Elizabeth Edgar. 2021. 'Ethical Principles for Artificial Intelligence in National Defence'. Philosophy & Technology 34 (4): 1707–29. https://doi.org/10.1007/s13347-021-00482-3.

Taddeo, Mariarosaria, Marta Ziosi, Andreas Tsamados, Luca Gilli, and Shalini Kurapati. 2022. Artificial Intelligence for National Security: The Predictability Problem. Centre for Emerging Technology and Security.

Taddeo, Mariarosaria, and Alexander Blanchard. 2022. 'A Comparative Analysis of the Definitions of Autonomous Weapons Systems'. Science and Engineering Ethics 28 (5): 37. https://doi.org/10.1007/s11948-022-00392-3.

UK Ministry of Defence (2021) Data strategy for defence: delivering the defence data framework and exploiting the power of data. https://assets.publishing.service.gov.uk/media/614deb7a8fa8f561075cae0b/Data_Strategy_for_Defence.pdf

UK Ministry of Defence (2023) Defence's response to a more contested and volatile world. London, UK. https://assets.publishing.service.gov.uk/media/64b55dd30ea2cb000d15e3fe/Defence_Command_Paper_2023_Defence_s_response_to_a_more_contested_and_volatile_world.pdf

United Nations High Commissioner for Human Rights (2021) The right to privacy in the digital age: annual report of the united nations high commissioner for human rights and reports of the office of the high commissioner and the secretary-general. A/HRC/48/31. United Nations Human Rights Council, Geneva, Switzerland

Watling J (2023) Supporting command and control for land forces on a data-rich battlefield. Royal United Services Institute

Weinbaum C, Shanahan JNT (2018) Intelligence in a data-driven age. Jt Force Q 90:4–9

Zhu L, Majumdar S, Ekenna C (2021) An invisible warfare with the internet of battlefield things: a literature review. Hum Behav Emerg Technol 3(2):255–260. https://doi.org/10.1002/hbe2.231