Afina, Yasmin; Grand-Clement, Sarah

Working Paper

Bytes and battles: Inclusion of data governance in responsible military AI

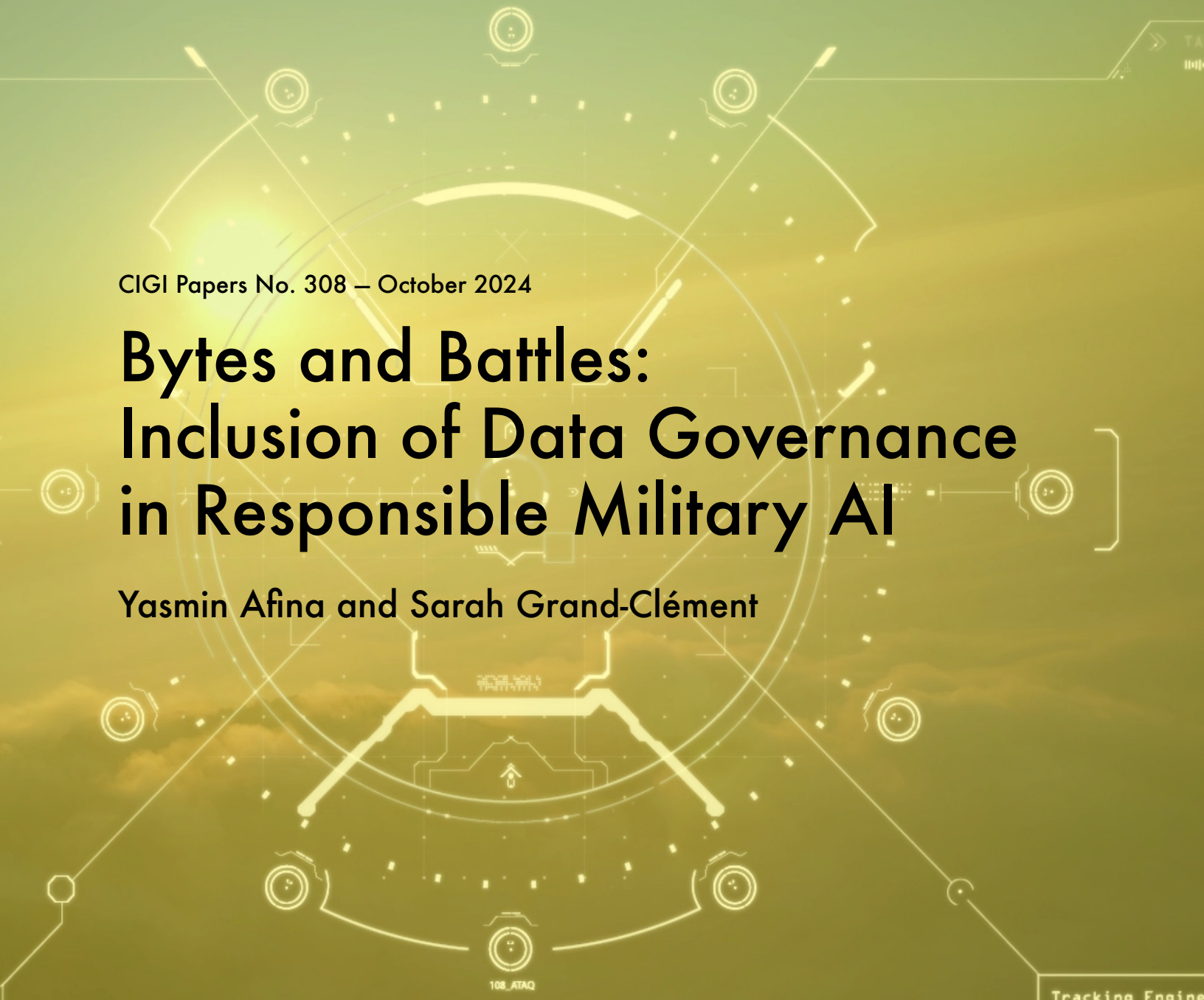
CIGI Papers, No. 308

Provided in Cooperation with:
Centre for International Governance Innovation (CIGI), Waterloo, Ontario

Suggested Citation: Afina, Yasmin; Grand-Clement, Sarah (2024) : Bytes and battles: Inclusion of data governance in responsible military AI, CIGI Papers, No. 308, Centre for International Governance Innovation (CIGI), Waterloo, ON, Canada

This Version is available at:
https://hdl.handle.net/10419/311774

Centre for International
Governance Innovation



CIGI Papers No. 308 — October 2024

Bytes and Battles: Inclusion of Data Governance in Responsible Military AI

Yasmin Afina and Sarah Grand-Clément

Centre for International
Governance Innovation

CIGI Papers No. 308 — October 2024

Bytes and Battles: Inclusion of Data Governance in Responsible Military AI

Yasmin Afina and Sarah Grand-Clément

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Managing Director and General Counsel Aaron Shull
Director, Program Management Dianna English
Program Manager and Research Associate Kailee Hilt
Senior Publications Editor Jennifer Goyder
Publications Editor Susan Bubak
Graphic Designer Sepideh Shomali

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

Table of Contents

vi About the Authors

vi Acronyms and Abbreviations

1 Executive Summary

1 Introduction

2 Data Governance: Taking Stock of Current Practices

6 Data Governance for Military Applications: Key Issues and Lessons from the Civilian Space

10 Key Legal, Policy and Ethical Implications of Dual-Use Nature of Data

14 Possible Policy and Governance Approaches to Data Practices Surrounding Military AI

18 Conclusion

19 Works Cited

About the Authors

Yasmin Afina is a researcher for the Security and Technology Programme at the United Nations Institute for Disarmament Research (UNIDIR), where her research covers the intersection between international security, international law and artificial intelligence (AI). Her research experience and interests cover nuclear weapons policy, outer space security, and wider international security and policy issues surrounding emerging technologies, including neurotechnology, quantum technologies and cyber.

Yasmin is also a Ph.D. researcher in law at the University of Essex. She holds an L.L.M. from the Geneva Academy of International Humanitarian Law and Human Rights, an L.L.B. from the University of Essex, as well as a French bachelor of laws and post-graduate degree (maîtrise) in international law from the Université Toulouse I Capitole. She previously worked as a research fellow at Chatham House, where she led the institute's work on AI policy, and notably testified in front of the UK House of Lords' AI in Weapon Systems Select Committee. Yasmin has published more than a dozen research papers, op-eds and commentaries on technology policy (including AI, cyber technology and neurotechnology) and nuclear non-proliferation and disarmament, and her work has been cited by a number of media outlets, including the BBC, *Politico* and Al Jazeera.

Sarah Grand-Clément is a researcher in both the Conventional Arms and Ammunition Programme and the Security and Technology Programme of the United Nations Institute for Disarmament Research (UNIDIR). Her work looks at the intersection of technology with conventional arms, exploring both the benefits that technology can bring to prevent violent conflict and enable peace, as well as the challenges and threats it can pose to international security. Sarah also has expertise in the use of futures methodologies as a way to help explore policy issues, in particular the use of horizon scanning, serious gaming and future scenarios. Prior to joining UNIDIR, Sarah was a senior analyst at RAND Europe, where she conducted research on defence and security issues for public and third sector policy making. She holds an M.Sc. in Arab world studies from Durham University.

Acronyms and Abbreviations

AI	artificial intelligence
CNIs	critical national infrastructures
GDPR	General Data Protection Regulation
ICRC	International Committee of the Red Cross
IHL	international humanitarian law
IHRL	international human rights law
PETs	privacy-enhancing technologies
RAISE	Roundtable for AI, Security and Ethics
REAIM	Responsible AI in the Military Domain
UNIDIR	United Nations Institute for Disarmament Research

Executive Summary

Data plays a critical role in the training, testing and use of artificial intelligence (AI), including in the military domain. Research and development for AI-enabled military solutions is proceeding at breakneck speed, and the important role data plays in shaping these technologies has implications and, at times, raises concerns. These issues are increasingly subject to scrutiny and range from difficulty in finding or creating training and testing data relevant to the military domain, to (harmful) biases in training data sets, as well as their susceptibility to cyberattacks and interference (for example, data poisoning). Yet pathways and governance solutions to address these issues remain scarce and very much underexplored.

This paper aims to fill this gap by first providing a comprehensive overview on data issues surrounding the development, deployment and use of AI. It then explores data governance practices from civilian applications to identify lessons for military applications, as well as highlight any limitations to such an approach. The paper concludes with an overview of possible policy and governance approaches to data practices surrounding military AI to foster the responsible development, testing, deployment and use of AI in the military domain.

Introduction

Data is the lifeblood of AI. The performance, effectiveness and overall reliability of AI systems are contingent on the quantity and the quality of the data that underpins their training and functioning. Essentially, data serves as the foundation upon which AI algorithms learn, adapt and perform their tasks. Beyond scientific research and evidence, there is growing recognition in policy, at the highest levels, of the importance and centrality of data in AI. On March 21, 2024, the United Nations General Assembly adopted a landmark resolution on seizing the opportunities and the promotion of "safe, secure and trustworthy" AI systems for sustainable development (United Nations General Assembly 2024). The resolution recognizes that "data is fundamental to the development and operation of artificial intelligence systems; emphasizes that the fair, inclusive, responsible and effective data governance, improving data generation, accessibility and infrastructure, and the use of digital public goods are essential to harnessing the potential of safe, secure and trustworthy artificial intelligence systems for sustainable development" (ibid., para. 7).

The importance of data governance has also been recognized by the United Nations High-level Advisory Body on Artificial Intelligence (2023) in its interim report, which includes a preliminary guiding principle on data governance, focusing in particular on the privacy and security of personal data. More broadly, the issue of data governance related to AI and the digital sphere is also a concern raised in the UN Secretary-General's "Our Common Agenda Policy Brief 5: A Global Digital Compact," which recommends the development of proper tools to avoid harms to individuals, communities and the global economy (United Nations 2023).

It is clear that as governments, civil society and industries grapple with the responsible development, deployment and use of these disruptive technologies, data will — and must — play a central role in AI governance. Military applications of AI are also dependent on data, yet this remains a severely underexplored issue in most, if not all, governance discussions and deliberations in this space; for example, none of the UN-led initiatives on data governance mentioned above focus on military applications of AI.

At the same time, discussions surrounding data are often shrouded with misleading assumptions that, in turn, could create or even amplify new and existing risks to compliance with international law (Holland Michel 2023). Left unaddressed, this issue could ultimately jeopardize the many commendable efforts promoting the responsible development, deployment and use of AI in

the military domain currently held within the auspices of the United Nations and beyond.[1]

This paper seeks to provide a meaningful contribution to the growing body of research underpinning governance discussions on military AI by examining the following questions:

- Why is data governance an important consideration for the military domain?
- How can AI data governance issues best be leveraged to promote responsible practices surrounding AI in the military domain?

In response to these questions, this paper has three objectives: provide a comprehensive overview of data issues surrounding the development, deployment and use of AI; examine data governance lessons and practices from civilian applications; and identify pathways through which data governance could be enacted. It is hoped that this paper can serve as a foundation for subsequent discussion and deliberation of how data-related issues can serve as a key intervention point to promote responsible AI in the military domain.

Data Governance: Taking Stock of Current Practices

A General Overview of Data Governance

In today's rapidly evolving world, data has emerged as a decisive factor in decision-making processes across all sectors. The importance of data lies in its ability to provide invaluable and often previously inaccessible insights, inform strategic planning and drive innovation. From the medical, agricultural and commercial sectors to the military domain, whoever harnesses the tremendous data being generated daily will maintain a competitive advantage (Cone and Luparello 2023). In a 2019 study, the World Economic Forum estimated that by 2025, 463 exabytes of data would be created each day across the globe (Desjardins 2019). Data can take many forms, including text, images, videos, sound, sensor readings and a combination thereof. Beyond the race to data supremacy, there is also growing recognition of the role data plays as a force for public good (The World Bank 2021).

The 2010s were marked by an explosion and frenzy around data: against a context of increased digitization and connectivity, the prospect of harnessing data for competitive advantage was most appealing. The term "big data" quickly became a buzzword — a common phrase as well as, quickly, the source of many concerns. Unrestricted access to (or at least very limited regulation of) personal data prompted organizations, agencies and individuals to establish a protective framework to safeguard fundamental rights and freedoms in the context of data practices. In 2012, the European Commission proposed a comprehensive reform of the European Union's 1995 data protection rules to consolidate online privacy rights; this eventually led to the adoption of the General Data Protection Regulation (GDPR).[2] Many have argued that the latter kicked off a "Brussels effect," with data protection regulations subsequently proliferating across regions, including in Brazil,[3] Thailand,[4] Nigeria[5] and China,[6] all reportedly drawing much of their inspiration from the GDPR. China has notably adopted a robust set of data governance structures, having identified data as playing an important role for economic growth. In parallel to the developments on data protection in the European Union, it has set up its own structures for regulating data, ensuring its security, and protecting personal information, through laws such as the Cybersecurity Law of 2016, and the Data Security and the Personal Information Protection Laws of 2021 (He 2023). While a deeper exploration of these case studies — and beyond — cannot be included in the present paper due to space constraints, further comparative studies on

1 For example, the United Nations Institute for Disarmament Research (UNIDIR) is leading, in partnership with Microsoft, a multi-stakeholder initiative, the Roundtable for AI, Security and Ethics (RAISE), aimed at promoting the responsible development, deployment and use of AI technologies in the security and military domains. Beyond the United Nations, the Netherlands and the Republic of Korea are spearheading processes surrounding the Responsible AI in the Military Domain (REAIM) Summit, first held in The Hague in February 2023. Following the summit, more than 50 states endorsed a common call to action. See Government of the Netherlands (2023).

2 See www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.

3 See DataGuidance by OneTrust and Baptista Luz Advogados (2024).

4 See OneTrust DataGuidance, OneTrust DataGuidance Regulatory Research and Blumenthal Richter & Sumet (2019).

5 See OneTrust Data Guidance (n.d.).

6 See OneTrust DataGuidance (2024).

data protection frameworks would be useful for both the policy- and law-making communities.[7]

One thing to note is that the obligations and rights provided by the GDPR may be restricted to safeguard national security, defence and public security, among others. Such restrictions, however, remain conditional insofar as they respect "the essence of the fundamental rights and freedoms," and that they are both necessary and proportionate measures.[8] As such, each use of data that may be in violation of the GDPR for security and defence applications must be justified through a test of necessity and proportionality in order to remain justified: in other words, these exceptions are on a case-by-case basis and cannot be subject to a blanket application.

Beyond data protection, the ecosystem of data governance frameworks has generally grown over the years. In 2013, Max Schrems, an Austrian lawyer, filed a complaint against Facebook Ireland Ltd., which subsequently led to a number of rulings both in Ireland and at the level of the Court of Justice of the European Union on privacy and cross-border data transfers (Batlle and van Waeyenberge 2024). Ten years later, the European Data Governance Act has entered into force, in recognition of the need to improve the conditions for data sharing and facilitating cooperation between EU member states, as well as the need to increase trust in data practices and in the "data economy."[9] This act embodies a more holistic approach to data governance, seeking to harness the transformative opportunities offered by data in the economy and in society, with safeguarding mechanisms in place. Similar regulations have also emerged, such as the US Clarifying Lawful Overseas Use of Data Act, which aims to facilitate data sharing in the context of criminal investigations.

AI and the Role of Data

Leveraging data, especially in light of its sheer scale, requires solutions to process it at speed and generate the desired outputs: AI holds tremendous potential to collect and utilize data. Once deployed, machine-learning systems can predict likely outcomes, calculate risks, draw insights and make sense of vast amounts of data otherwise unattainable to human analysts and at speed (Deeks, Lubell and Murray 2019). To this end, however, these technologies will need to learn from data to recognize and identify patterns and trends, to make predictions and, subsequently, to generate outputs. As such, data plays a critical role across the life cycle of an AI technology. From its training to its deployment and use, data is not a static and passive input: it is a dynamic force that shapes the AI technology's development, performance and evolution over time.

Data also plays a critical role in the testing, evaluation, verification and validation of AI technologies. For instance, as AI models go through test cases that cover different scenarios and edge cases, testing data will be essential to represent the conditions under which the systems are intended to be deployed. These tests can take the form of adversarial methods using inputs designed to mislead and "fool" the model. Developers will then analyze how the system responds to adversarial examples against training and validation data, which, in turn, will help identify vulnerabilities in the model. Data will also play a central role for regression testing, to ensure that recent changes, tweaks and modifications to the AI system and its parameters have not introduced new bugs or "regressed" its performance (Orso, Apiwattanapong and Harrold 2003).

Once AI models have gone through testing, evaluation processes will measure their performance and their outputs against a set of metrics and indicators. Benchmark data sets are generally used to compare and evaluate the outputs produced by the model, providing a standardized basis across various tasks. This will then be complemented with real-world data for the contextual evaluation of the models, thus providing insights into their performance under actual operating conditions. In the medical and health-care sector, for example, real-world data (for example, patient health status, delivery of routine health care) is used to evaluate the performance of AI-enabled solutions, thus

7 There is a rich and growing body of literature looking at the various approaches to data protection across the globe; the authors of this paper simply cannot do justice to the many nuances and intricacies of research in this space due to space constraints and have thus elected not to elaborate further than what is discussed here.

8 EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*, [2016] OJ, L 119/1, art 23.

9 EC, *Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)*, [2022] OJ, L 152.

bridging the gap between clinical research and practice (Liu and Panagiotakos 2022).

It is also important to note that, prior to being integrated and used in the development, deployment and use of AI technologies, data generally goes through a number of processes and practices. Box 1 provides some terms and processes that should be considered in the context of this paper, although they in no way constitute an exhaustive list of data practices adjacent to the use of data for AI development.

Box 1: Data Practices

- **Data collection:** Data collection is the process of retrieving and gathering existing data for a pre-defined purpose. Three considerations frame and shape data collection practices: the type of data needed, the source(s) and methods of collection.
- **Data generation:** This process refers to the creation or production of new data through various means, such as sensors and experiments, as well as simulations and models. The data generated can either be intentionally produced for a specific purpose or it can be naturally generated through external and various processes.
- **Data cleaning:** Once data has either been collected or generated, it must go through a number of processes to ensure its quality by identifying, correcting, and/or removing undesirable data. In other words, it consists of "cleansing" the data of errors, inconsistencies and inaccuracies that are either irrelevant for the defined purpose or can even jeopardize the system's calculations and outputs.
- **Data hygiene:** Once the data has been cleansed, certain practices and processes must be in place to maintain the quality, accuracy, consistency, suitability and continued relevance of the data for its intended purpose and throughout its life cycle.
- **Data security:** In addition to data hygiene practices, a number of processes must be undertaken to ensure the data's security and promote privacy protection through encryption, data masking and anonymization (if appropriate).
- **Data labelling:** Depending on its intended use, data will also go through the assignment of descriptive tags, categories or annotations. This step is particularly essential for supervised machine learning.
- **Data processing and use:** Once ready, the data can be used to generate insights and inform decision-making processes through its analysis, interpretation and application.
- **Data storage:** Data, while intangible, must be stored and will involve physical and digital infrastructures (for example, databases, cloud storage, servers). Security measures must be in place to ensure the data's protection from unauthorized access, loss or corruption (for example, through data poisoning).
- **Data transfer:** Data can be moved from one location to another, either within the same system or between different systems or networks. The implications of cross-border data transfer have been of particular interest in national security and law enforcement contexts.
- **Data archiving:** Once of no active use, data can be retained and preserved long term, for example, for compliance purposes, historical reference and/or future analysis.
- **Data deletion:** Data can also be permanently removed from storage systems. Deletion may be necessary, at times, for compliance purposes (for example, data privacy laws).

Discussions on data are crucial for the development of governance pathways. Understanding the many processes underlying the collection, processing, use and management of data will help identify critical intervention points and solutions to address both the underlying risks stemming from data practices and those from the development, deployment and use of AI in the military domain. Ultimately, promoting responsible AI in the military domain will require robust discussions on data governance to ensure that AI systems are developed, tested, deployed and used in accordance with international law, ethics and applicable policies and standards while promoting such compliance.

Data Governance Frameworks and the Advent of AI

In addition to general-purpose regulatory frameworks akin to the GDPR, a number of data governance approaches and practices tailored to address sector-specific issues have emerged. Different sectors — including the financial domain, digital platform regulation, health-care provision, and humanitarian and disaster relief — raise unique issues and concerns that require targeted solutions. As a result, guidelines, handbooks, policies and other types of "soft law" frameworks are gaining in number and prominence. These instruments, too, increasingly recognize the interlinkages between data and AI governance.

In the case of the humanitarian sector, organizations working in this space deal with the highly sensitive personal data of vulnerable communities in volatile environments. The International Committee of the Red Cross (ICRC) has issued a *Handbook on Data Protection in Humanitarian Action*. Already in its second edition, it "builds on existing guidelines, working procedures and practices" and has identified AI as one of the key issues for data protection.[10] While the intersection between AI and data remains very much underexplored in the humanitarian context, calls for concrete approaches and solutions to address the issues it raises are growing (Spencer 2024). As outlined in the handbook, AI is being used to facilitate humanitarian work and activities linked to it, including to read public opinion, identify and locate missing children, track attacks on civilians and human rights violations, as well as to prevent and diagnose disease. While these technologies offer opportunities, AI applications also pose challenges: beyond data protection concerns, the accuracy and reliability of systems can jeopardize the conduct of humanitarian work and have severe repercussions on civilians. For instance, off-the-shelf solutions, while less costly and more accessible, carry risks with regard to the systems' predictability and reliability. Humanitarian action often requires a tailored and targeted approach due to the complexity and intricacies of individual crises (for example, cultural factors, demographic realities, local environment and climate).

Another key example corresponds to data governance frameworks in the context of AI integration for critical national infrastructures (CNIs). There is evidence that AI is indeed playing an increasing role in society — including across all spectrums of CNIs, from the provision of energy supply to finances, communications and "smart cities," as well as the security and defence sector (Gerstein and Leidy 2024). AI innovation holds tremendous potential in supporting CNIs, yet it also raises a number of novel and long-standing issues and questions. For instance, while the integration of (and increasing reliance on) generative AI into critical functions and infrastructures exacerbates pre-existing digital and physical vulnerabilities (for example, the targeting of computing power and infrastructure), it also raises novel concerns (for example, the corruption of training data through data poisoning, as well as the hijacking of model output) (Department for Science, Innovation & Technology 2023). Beyond wider security concerns, the integration of AI into CNIs also raises data-related concerns: from risks of data leaks to biased systems compromising human decision making, it is clear that further research, and deeper reflections on data governance approaches and solutions, in the context of AI integration in CNIs is a sine qua non condition for a responsible AI ecosystem (Electric Power Research Institute 2020). As such, while falling outside of the military domain, the development, adoption and integration of AI solutions add further layers of complexity to ensuring the security and resilience of CNIs, for which data plays a key — yet underexplored — role.

Data in AI Governance Frameworks

As AI governance frameworks mushroom across the globe, it is clear that data plays an important role in forming this dynamic and ever-evolving

10 See www.icrc.org/en/data-protection-humanitarian-action-handbook.

policy landscape. Data lies, for instance, at the heart of the Executive Order on Safe, Secure and Trustworthy AI issued by the White House in late 2023.[11] It highlights the need to safeguard the right to privacy against the mass use of data to train AI systems, while prioritizing the development and use of privacy-preserving techniques, including those that are AI enabled.[12]

Similarly, data also features prominently in the newly adopted EU AI Act. The EU AI Act recalls, in fact, the 2019 *Ethics Guidelines for Trustworthy AI* developed by the High-Level Expert Group on AI, which was appointed by the European Commission and identified "privacy and data governance" as one of the seven key principles underpinning trustworthy and ethically sound AI. The act asserts the vital role high-quality data and access to high-quality data play in providing structure, and in ensuring that high-risk AI systems perform as intended and safely and that they do not become a source of discrimination.[13] Article 10 of the act is specifically dedicated to "data and data governance." It includes provisions on the training of high-risk AI systems and adjacent practices surrounding their development, including data-preparation processing operations, the formulation of assumptions, and the adoption of appropriate measures to detect, prevent and mitigate possible biases.[14]

The EU AI Act generally excludes from its scope AI applications for military, defence or national security purposes. However, it is also important to note that when AI systems are developed, placed on the market, put into service and used for such purposes, but are used "outside those temporarily or permanently for other purposes, for example, civilian or humanitarian purposes, law enforcement or public security purposes," these systems would fall within the scope of the act.[15] In other words, dual-use technologies fall within the scope of the EU AI Act when not in use for military, defence or national security purposes. The implications of the act, once entered into force, on data practices surrounding dual-use systems should be unpacked in further detail in a subsequent dedicated study.

Data Governance for Military Applications: Key Issues and Lessons from the Civilian Space

Data for Military Applications

Data has also increasingly been recognized as a key asset by militaries, as demonstrated by the various dedicated policies and strategies, such as Canada's 2019 *The Department of National Defence and Canadian Armed Forces Data Strategy*,[16] the United Kingdom's 2021 *Data Strategy for Defence*,[17] the United States' 2023 *Data, Analytics, and Artificial Intelligence Adoption Strategy*[18] and the Netherlands' 2023 *Defense Strategy Data Science and AI 2023–2027*.[19] Table 1 provides an overview of the key principles that form the Canadian, Dutch, British and US data strategies.20 It should also be noted that the topic of data is, at times, subsumed in other defence-related policy documents or strategies. For example, France's 2019 *Artificial Intelligence in Support of Defence* report notably places an important emphasis on data, stating that it is one of the "necessary foundation[s] for the successful development of AI" (AI Task Force 2019), despite the strategy itself not being solely focused on data.

11 See The White House (2023).

12 On privacy-preserving, or privacy-enhancing technologies (PETs) and data privacy, see Inverarity (2023).

13 EC, *Regulation 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)*, [2024] OJ, L 12.7 at para 27.

14 *Ibid*, art 10.

15 *Ibid* at para 24.

16 See The Department of National Defence and Canadian Armed Forces (2019).

17 See Ministry of Defence (2021).

18 See Department of Defense (2023).

19 See Department of Defense (Netherlands) (2023).

20 Many more countries, including from the Global Majority, have general strategies focused on digitalization, data or AI that are cross-government in nature. However, this comparative table is intended to showcase countries' strategies or policies on data specifically in the military domain and that are publicly available, hence the limited number of countries featured, all of which are Western. To date, very few countries have strategies that focus specifically on the military domain.

Table 1: Comparison of Canadian, Dutch, UK and US Data in Military Strategies

Canada	Netherlands	United Kingdom	United States
→ Data is a shared asset → Data is accessible → Data is secure → Data is trusted → Data is managed ethically	→ Defence-wide data governance → Advanced information technology → Investing in knowledge and skills → Data-driven way of working	→ Exercise sovereignty over data, including accountability and ownership → Standardize data across the defence landscape → Exploit data at the most effective and relevant point in the value chain → Secure digital data at creation, curation, when handling, storing and transmitting → Curate data, ensuring it is assured, discoverable and interoperable → Ensure data as an asset beyond individual projects	→ Visible (i.e., necessary data can be located) → Accessible (i.e., necessary data can be retrieved) → Understandable (i.e., data can be understood) → Linked (i.e., relationships between data are maintained) → Trustworthy (i.e., users have confidence in the data) → Interoperable (i.e., data can be exchanged between systems and users) → Secure (i.e., data is appropriately safeguarded from unauthorized use or manipulation)

There are a number of similarities between the principles present in the four strategies, namely around the importance of data security, the accessibility and usability of data by different users and the trustworthiness of data. While these do not discuss the specifics of data practices outlined earlier in the section "AI and the Role of Data," there are nonetheless references to some of these practices within the strategies. For example, the United Kingdom's strategy encapsulates a number of these practices, from data creation and its archiving and deletion, under the term "data standards," which it states should be leveraged and adhered to by all personnel. However, even the most recent of strategies, those of the United States and the Netherlands, note that policies are still required on some of the aforementioned data practices, such as their labelling.

Currently, only a minority of states have produced a specific data strategy focused on the military domain, and even fewer have a strategy focused on data for AI systems specifically. It is nonetheless important to note that the distinction between a strategy pertaining to data in the military domain, with mentions of AI, is not equal to a strategy aimed at data for use in AI. This distinction is important, as AI data governance differs from traditional data governance, in that the former considers the role and impact of AI algorithms on the data itself, and the evolutive nature of AI, in addition to the concepts contained within "traditional" data governance (Chu 2024).

But why such a focus on data within the military domain? Why do the recent strategies for France (2019), the United Kingdom (2021) and the Netherlands (2023) consider data a "strategic asset"? Information and data have always been relied upon

in the military context to make decisions. These can range from recruitment of personnel and logistics planning (for example, helping decide which assets can be deployed and their most optimal routing), to management and decision making in the context of military operations. This has become even more critical with the advent of digital technologies, the increased use of sensing technologies and the digital transformation of the military domain. The adoption of these technologies has increased the possibilities of data use and, as such, enhanced the value of data for military decision making, both within the context of military operations and more broadly for the conduct of supportive activities. At the same time, as data production and the amount of data available has increased, so too has the need to sort out relevant data from the "noise."

This is one area where AI can add value. It can enable even greater value to be generated from existing data and data sources and their use within the military context. Specifically, the use of AI could help overcome human cognitive limitations linked to information overload, and could ensure that information valorization is made less time- and labour-intensive (Meerveld et al. 2023). AI capabilities and their relevance are multi-faceted; AI could help military decision making and planning and the conduct of military action, and improve the efficiency and resilience of supporting activities.

While the use of AI within weapon systems to aid with targeting and engagement of the target, referred to as downstream military tasks,[21] is a topic that has already been and continues to be discussed at length in multilateral fora and beyond,[22] the application, both actual and potential, of AI goes far beyond this narrow scope. Due to AI's ability to sort through and help analyze large amounts of data, as well as to identify patterns and relationships in the data, it can help make calculations, predictions or forecasts, generate recommendations or create a large range of simulations of future actions or outcomes. Specifically, AI can help undertake different functions of a military operation, from command and control tasks, which include assessing weapon capabilities and effects or planning battlefield manoeuvres; information management, which includes analyzing intelligence, surveillance and reconnaissance data and managing information and communication security; logistics, which includes assessing the operational effectiveness of people and equipment; and training of military personnel.

Currently, a wide range of AI capabilities are already technically feasible and are employed in the military context — from ship maintenance (Africa Defense Forum 2023) to target recognition (Nurkin and Siegel 2023; Abraham 2024) — but many more are projected to be not only feasible but also desirable. This pertains, in particular, to enhanced ability for cross-domain, cross-service and cross-spectrum interoperability and data fusion (Grand-Clément 2023; Eversden 2020). Overall, while drawbacks, challenges and risks to using AI in the military domain have been highlighted and acknowledged,[23] its further integration in the military domain continues. As such, the importance of data grows in parallel to the increased use and potential for use of AI in both upstream and downstream tasks.

Data in the Military Domain: Key Issues

There are limitations to the use of data for AI capabilities. On the one hand, some of these limitations or challenges can be found in both the military and civilian domains, such as:

- **Real-time situation versus historical data:** AI models will be trained with historical data (or data that has been synthetically created based on historical data). However, when a model is eventually used, the situation in the real world may no longer accurately reflect the data a model has been trained on, a condition called "distributional" or "prediction" drift (Schraagen 2023).
- **Biased data sets:** This issue is perhaps the most well-known and frequently discussed with regard to data for military AI. The risk that there can be biases within data sets is already acknowledged, notably in how gendered, racial, societal or other biases and discrimination that

21 Downstream military tasks are those that pertain to tasks on the "visible end" of military decision making, namely, to target selection and target engagement. This is opposed to upstream military tasks, which occur prior to the downstream tasks and include activities that have an "indirect effect of lethality." See Grand-Clément (2023) and Ekelhof and Persi Paoli (2020).

22 See, for example, Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System (2023) and Nurkin and Siegel (2023).

23 See, for example, Grand-Clément (2023), Puscas (2023) and Scharre (2019).

exist in the real world could be reflected in the data (for example, "all military personnel are men of a certain age," or attributing more importance to the occurrence of a particular event than there is in reality). In the military domain, biased data sets could lead to faulty decision making, which could also cause violations of international humanitarian law (IHL).[24] Such biases can be replicated by models that are trained with this data and eventually could exhibit these biases in their outputs (Chandler 2021; Bode 2024).

- **Incorrect data:** Data can be incorrect or falsified in various ways, beyond the issues of biases and inaccuracies in time described above. For example, it could have been unintentionally mislabelled; equally, it could have been intentionally poisoned or otherwise manipulated in order to induce a model into error.

On the other hand, data in the military domain has certain particularities that sets it apart from the civilian one in certain respects. The following issues may also be relevant for non-military applications of AI, but they have particular nuances and variations that are specific to the military domain:

- **Data availability:** Military operations usually involve working jointly with a range of stakeholders, which includes different services, other militaries and governments, as well as contracted private sector entities. This means that relevant data can be fragmented and owned across these different actors, who may transform and use the data in different ways, and with specific parties who may not want or be able to relinquish proprietary data. The data may have been processed following varying standards and, as a result, may pose issues not only with regard to interoperability but also to security. In fact, sensitive data may be classified and secured (for example, encrypted) in various ways, which can hamper the ability to use or even share such data between relevant stakeholders, whether for training purposes or real-world use (Lin-Greenberg 2020).

- **Amount of training data:** Data specific to the military domain is more limited and more difficult to obtain. This issue is relevant both with regard to the sheer quantity of training data and the lack of quality training data sets. Data sets that are too small can have an impact on the ability to train, test and use a model, which will likely be underfitted or "too simple" due to the lack of training data. As such, the reliability of AI systems intended to undertake complex tasks (for example, decision support systems will need to factor in legal compliance and thus cannot be oversimplistic in light of IHL's many nuances) will suffer, which, in turn, can have serious consequences for mission success and legal compliance. An AI model might, for example, be obliged to create more inferences, thus leaving more room for false or misguided interpretations. Actors within the military domain and beyond have examined avenues to mitigate this challenge, such as by using synthetic data. While this does offer benefits and can help broaden the availability of training data, it also comes with risks, such as not being able to sufficiently replicate the real world, or can even degrade the performance of an AI system (Deng 2023). This example raises many issues that stem from the lack of quality of training data sets: vast amounts of training data would not be enough — they must also be of good quality and as well as having gone through the many data hygiene and security processes discussed earlier, they must also be adequate for the inherent issues the system is set to address. Quantities of training data from past operations in one location may come in handy, but will not be reflective of local contexts and realities for future operations in other places. For example, a computer vision program may be trained to classify individuals as combatants based on the bearing of arms, which may be accurate in certain regions but may be a local, cultural custom among civilians in other parts of the world. There are many reasons for insufficiencies in data, including struggles some armed forces face with the digitization of their historical records from past military operations and the sensitivity around this data. These issues both hamper the design and training of AI-enabled capabilities and constitute an obstacle to their responsible development and subsequent deployment and use.

It should also be noted that the risk is not equal to all types of models and all types of situations. For example, there may be a greater abundance of data, with limited biases (or possible impact of such biases) in certain areas — such as on predictive equipment maintenance or logistical routes —

24 If the training data sets relied on past operations in another part of the world with different demographic realities, the system may erroneously associate certain ethnicities with combatant status. See Afina (n.d.).

versus others, such as calculation of civilian patterns of life or target identification. These issues also do not take into account other factors, such as the fact that the current data collection processes used by militaries may not be adapted for use by AI models (Svenmarck et al. 2018).

In light of the high stakes involved, these issues and nuanced considerations must be included in data governance deliberations and discussions. Data governance constitutes a key and decisive element in enabling responsible AI in the military domain.

Key Legal, Policy and Ethical Implications of Dual-Use Nature of Data

Data's Dual-Use Nature

AI being a dual-use technology has been at the forefront of many discussions and debates. Yet there is also a need to examine the dual-use nature of data. Some data may concern civilians and civilian infrastructure and be used in a military context; equally, some data may be intended for civilian applications, but eventually be used for military purposes. This aspect of dual-use data is particularly salient in light of the blurring of the lines between the military and civilian domains, as well as in terms of the limitations in the amount of military data available.

There are three main aspects to consider with regard to the use of dual-use data in military AI:

- The entities that develop, train and test the AI models for use in the military domain. These are predominently non-state actors, particularly industries. Therefore, a key question is whether these entities have sufficient access — both in terms of quantity and quality — to relevant military data to train the models, taking into account the issues on access and availability discussed above.
- The type of data being used to train the models (and whether it is pertinent) and, overall, the traceability of the data's source(s), collection methods, motivations and parameters surrounding collection and processing practices, data hygiene processes, and so on.
- The type of data that is then fed into the models once operationalized. Questions to consider here are whether issues of data cleaning, data hygiene, data labelling and more are conducted — at all — given pressures of the operational environment (for example, the need to maintain a rapid pace), but also whether these aspects take into account dual-use data issues in an operational context.

"Civilian" data is not homogenous; there are different categories or subsets of such data. Three of these subsets come under consideration within this paper. The first is data that concerns civilian objects, is civilian in nature (or is not inherently military) and that is used in a military context — such as data on weather conditions, geographical data or data about civilian infrastructure. The second pertains to data on military personnel taken from a civilian data source — such as social media platforms. The third is personal data on civilians, taken from civilian sources (for example, the interception of Global System for Mobile Communications data).

This approach to using dual-use data and its applications has been increasingly noted, in particular, in the context of certain recent and ongoing conflicts, as several examples demonstrate. In 2022, US company Clearview AI, which originally was used by law enforcement authorities in the United States, made headlines when it was reported to have provided Ukraine's armed forces with facial recognition technology to identify the dead, as well as refugees and Russian military personnel. The system is reported to be trained on more than two billion images from a Russian social media platform, VKontakte, with some reports also suggesting that Meta has requested that Clearview AI stop taking its data.[25] Additionally, the Ukrainian military, aided by civilian defence technology company Palantir, has used data posted on social media by Russian soldiers, and other open-source data, to identify targets (King 2024).

Another recently reported use case of civilian data used to inform a target identification program involves Israel's Lavender system, which allegedly uses data from Meta's WhatsApp and other sources

25 See Dave and Dastin (2022); see also Bhuiyan (2022), Hern (2022) and Meacham and Gak (2022).

in the context of Israel's military operation and attacks in Gaza (Arab News 2024).[26] Meta has, however, denied the claims, specifically stating they have no information that these reports are accurate. Conversely, the Israel Defense Forces released a note in June 2024 on its use of data technologies in intelligence processing — including the Lavender system.[27] The veracity and accuracy of both of these claims cannot be independently verified; it is, however, clear that as use cases of AI technologies in the military domain increasingly surface, public scrutiny over the use of civilian data to train these systems will only grow in magnitude, and clarity on the legal and ethical implications of such practices will be required. There is therefore a pressing need to tread carefully and ensure discussions are based on evidence and remain grounded to avoid risks from over-hype.

Overall, the underlying enabling structures and mechanisms — in this instance, data — of the civilian and military domains are closely intertwined. This blurring of lines between civilian applications and practices, on the one hand, and the military domain, on the other, subsequently introduces a host of legal, policy and ethical implications.

Many of these stem from the complex, multi-layered and multi-staged nature of data practices surrounding the development, training and testing of AI technologies. Challenges arise with regard to the assessment and verification of the training and testing of data sets' quality, which, ultimately, will have an impact on the reliability and performance of the AI system in question. For example, the use of open-source data, or the purchase of proprietary commercial data, induces traceability and transparency issues, which stand in the way of verifying its quality; such practices also open up military actors to potential vulnerabilities (Goldfarb and Lindsay 2022).

The inability to trace the sources of training data, in addition to the underlying motivations, collection methods, surrounding parameters and assumptions, as well as the context in which such data has been collected, all raise challenges with regard to legal compliance. For instance, left unaddressed, harmful biases present in commercial "civilian" data used to train military applications can have serious consequences on implementing the rule of distinction. Perhaps one of the most prominent examples concerns the racial bias present in Google Vision Cloud, exposed by AlgorithmWatch in 2020 (Kayser-Bril 2020). The system would, essentially, label the image of a dark-skinned hand holding a temperature-measuring "thermogun" as that of a "gun," while the same image with a fair-skined hand would be labelled as "electronic device." If the same system was used to inform AI-enabled systems for target recognition, there is a high risk that it would misidentify dark-skinned civilians as directly participating in hostilities (and thus, as targetable) simply due to their skin colour. This example demonstrates not only the importance of identifying and addressing harmful biases in the training data sets underlying military AI but also the need for training data sets to be traceable, especially in light of the growing tendency to use civilian data to feed into military applications.

Legal Implications and Issues

Beyond biases, a series of additional legal issues may arise from this "entanglement" of civilian data with the development, deployment and use of AI in the military domain. One of these questions pertains to the applicability (and subsequent application) of regulatory instruments primarily aimed at "civilian" applications, which, by nature, are of dual use and thus raise uncertainties as to how they should be applied. In the case of the GDPR, for example, and as discussed earlier, it is clear that the processing of data for security and defence purposes can exempt states from the obligations set forth in the regulation, provided it satisfies the tests of proportionality and necessity. Yet this exemption applies on an exceptional and case-by-case basis, which contrasts with the need for data en masse required to develop, train and test AI systems. In addition, in the case of the EU AI Act, its applicability and subsequent application are even more convoluted: while the latter generally aims to exclude security and defence from its scope, the act applies in situations where systems were originally designed for such applications but are temporarily used for civilian purposes (for example, for humanitarian relief). As such, the applicability of the EU AI Act on dual-use technologies is yet to be further examined and clarified — a particularly important task as the Brussels effect is being tested and non-EU states are looking into modelling their own regulatory instrument after the act.

26 See also Middle East Monitor (2024).

27 See Israel Defense Forces (2024).

Furthermore, the use of personal data of civilians also raises issues vis-à-vis compliance with international human rights law (IHRL), the violation of which places them at increased risk of undue harm by including this data in military data sets without the appropriate safeguarding measures and mechanisms in place. In fact, beyond the applicability of international humanitarian law in armed conflict, IHRL complements the latter, in addition to during peacetime. In 2021, the United Nations High Commissioner for Human Rights released a report on "the right to privacy in the digital age." A section is dedicated to AI use in law enforcement, national security, criminal justice and border management — all applications that may equally be used in the military domain, especially in contexts where the armed forces are deployed to combat organized crime.[28] The report presents a number of use cases where states are increasingly integrating AI systems for said applications, including as forecasting tools, biometric recognition, as well as "predictive biometrics," that is, to allegedly decide whether someone is a security threat based on their deducted emotional and mental state (United Nations General Assembly 2021, para. 22–28). These applications are all known to require vast amounts of data for training and functioning — often sensitive personal data such as criminal records, communications data and travel records. A number of human rights implications are then laid out in the report, including on the rights to privacy, to a fair trial, to freedom from arbitrary arrest and detention, and the right to life. The implications of AI on these rights are, in fact, increasingly and extensively scrutinized within the Human Rights Committee.[29]

Finally, the use of civilian data to feed into military AI's outputs raises questions with regard to the implementation of IHL's rule of distinction. The latter essentially differentiates between lawful targets (that is, "combatants" and "military objectives"), and unlawful targets (that is, "civilians" and "civilian objects"). One long-lasting contentious point in international law is the case where civilians lose their protection from direct attack, that is, when they are engaging in "direct participation in hostilities." The ICRC defines the direct participation in hostilities as when persons "carry out acts, which aim to support one party to the conflict by directly causing harm to another party, either directly inflicting death, injury or destruction, or by directly harming the enemy's military operations or capacity" (ICRC 2009). In studies involving the conduct of cyber operations, a number of research efforts have been dedicated to examining how to interpret this already contentious status in the digital realm.[30] In the context of the war in Ukraine, the government's Diia app has been repurposed to allow users to report and inform the Ukrainian Armed Forces of movements of invading soldiers; however, it has been argued that the use of this app puts civilians at risk of losing their protection from attack, as they may be considered as directly participating in hostilities (Olejnik 2022). While these examples do not necessarily pertain to AI applications, the issues presented are very much relevant. If, for example, an AI system is used for intelligence collection to scan messages sent on social media platforms, to identify civilians directly participating in hostilities, the extent to which a civilian's messages can "incriminate" them remains unclear. There is thus a need for established guidelines to safeguard due process and human rights, while also factoring in the present realities in warfare and the use of AI to enhance intelligence collection and processing.

These issues, while non-exhaustive, are onerous enough already for the authors to establish that there is an urgent need for further research and efforts to address data practices to promote the responsible development, deployment and use of AI in the military domain. The time-sensitive nature of this task is further amplified by the growing tendency, or at least interest, from states to procure off-the-shelf capabilities.[31] Concurrently, industries may feel more inclined to rapidly develop and commercialize these tools. For certain applications, this may very well be appropriate. Yet, in many cases, the sensitive nature of warfare, in addition to the need for the system to align to the procuring armed forces' internal strategies, policies, decision-making habits and values, will require bespoke solutions. Their design, development and training will subsequently require data sets tailored to the client's operational needs, parameters and military culture, as well as internal policies and strategies — all of which cannot be

28 In Latin America, for example, states are increasingly deploying the military in their approach to combat organized crime. See Schenoni and Madrid (2024).

29 See, for example, United Nations Human Rights Committee (2019, 2020).

30 See, for example, Wallace, Reeves and Powell (2021).

31 See, for example, UK Army (2023).

compromised in order to ensure the reliability, safety and security of the procured system.

Lessons from Data Governance in Non-military Contexts for Military Applications: Opportunities and Challenges

Research and subsequent deliberation on data governance in the context of AI in the military domain remain in early stages, with much yet to unearth. However, as data governance efforts and thinking in non-military contexts are reaching remarkable levels of maturity, a number of opportunities for cross-pollination with the military domain should be considered. This includes both governance approaches and proposed solutions for operationalization, for example, through data hygiene practices, the translation of legal and ethical frameworks into technical requirements, as well as the conduct of red-teaming and adversarial exercises to stress test the model in question. Careful consideration ought to also be given to the highly sensitive and, more generally, the inherently different nature of military applications. The latter will require that careful consideration is infused into all data governance approaches and solutions for military applications.

With regard to opportunities for cross-pollination, data governance approaches, efforts and even frameworks in the civilian space have reached the point where they can provide some insights and lessons for the military domain. Some best practices to ensure data hygiene can, for example, be drawn from the civilian sphere and applied in the military domain. This could be by ensuring human oversight on data collection and use to monitor and eventually, if need be, respond and address "inaccurate, unfair, or discriminatory results" as early as possible in the process (Houser and Bagby 2024). In situations where there is insufficient training data, the military domain could also draw lessons from what is considered as a purpose-driven approach to data collection, that is, "the production and availability of a sufficient amount of reliable and accurate…data that is suitable to be the 'experience' with which a machine can be trained" (Cabitza, Campagner and Balsano 2020). In other words, this approach is ensuring that developers are mindful of the adage "garbage in, garbage out" (Kilkenny and Robinson 2018), and exercise caution to ensure the quality of the training data from the early collection stages. This approach ought to also be socialized, adopted and widely implemented in the military domain. Given the high stakes of military AI use, especially with regard to decision support systems, if they had been trained on "garbage," there is a risk that the resulting garbage output is considered and accepted as proper and accurate advice, which may result in the violation of international law and ethical requirements.

Another paradigm the military domain could learn from corresponds to that of law enforcement. There has been extensive research by international organizations in the context of promoting responsible AI innovation, deployment and use to support law enforcement agencies. In a recent study, for example, the Centre for Artificial Intelligence and Robotics at the United Nations Interregional Crime and Justice Research Institute, in partnership with Interpol, laid out four principles as part of their Responsible AI Innovation in Law Enforcement tool kit: lawfulness, minimization of harm, human autonomy and fairness (United Nations Interregional Crime and Justice Research Institute and Interpol 2024). The minimization of harm consists, among other things, of ensuring the accuracy of AI systems, which requires careful consideration for the origin and composition of the training data, both when procuring an AI system or developing it internally (ibid., 12). In addition, and as discussed above in the section "Data in the Military Domain: Key Issues," there have been extensive discussions within the United Nations with regard to the human rights implications of developing, deploying and using AI technologies in law enforcement operations. Given the overlapping security considerations between law enforcement and the military domain, in addition to the trend, in certain regions, of increasing militarization of law enforcement operations, there is tremendous potential for cross-pollination and mutual learning to support responsible data practices.

Due to space limitations in this paper, the authors are not able to explore in further depth and detail the many other instances where the military domain could draw lessons from data governance approaches in non-military contexts. It is, however, important to note that while cross-pollination and mutual learning are important, it is also critical that analysts, policy makers and practitioners are mindful of the inherently sensitive nature of the military domain. This, subsequently, poses limitations on the ability to transcribe lessons and approaches from the civilian into the military

realm. One such example is that of "informed consent," a process in the medical field whereby a health-care provider informs and educates the patient about a given procedure or intervention, including its risks, benefits and alternatives (Shah et al. 2023). In the same vein, governance efforts to foster data equity in the civilian space are seeking to adopt a similar approach.[32] Yet in the military domain, while transparency lies at the heart of efforts and initiatives to promote responsible AI practices, it cannot be approached in the same manner as that of informed consent due to the sensitive nature of operations and data. This is just one of the many possible examples to illustrate the limitations stemming from the inherent differences between the civilian and the military spaces, which would merit further research in a subsequent study beyond this paper.

Possible Policy and Governance Approaches to Data Practices Surrounding Military AI

As shown throughout this paper, the question of data governance in the context of AI is critical and, to date, severely overlooked. It is therefore important to not only pay greater attention to this question, but also to consider the appropriate governance fora and pathways to enable progress in this space. These reflections must acknowledge and consider the complex, multi-layered and multi-levelled nature of data (that is, not all data is equal); the various possible uses of data across both military and non-military domains; and data's respective governance parameters (that is, conditions under which it should or should not be included in governance discussions and frameworks on military AI). As such, a number of possible approaches for operationalization are emerging and subsequently presented in this section, some of which build upon the work that has already commenced within some of the already published national strategies and policies on data in defence and AI data in defence, as well as broader initiatives and frameworks not encompassed within these strategies.

Public-Private Collaboration and Cooperation

There is evidence of the benefits of enabling inclusive and meaningful multi-stakeholder cooperation to support and advance AI governance, including in security and defence.[33] Held at the international, regional and national levels, such platforms can bridge the perspectives of public and private sectors across disciplines and geopolitical divides, and establish trust and, ultimately, a strong foundational basis for meaningful progress. These dialogues can, in fact, provide the space required to gather stakeholders, dissect the many building blocks of AI, and ultimately develop concrete policy recommendations and solutions to advance the responsible development, deployment and use of AI in the military domain. A dedicated space for governance discussions, information exchange, knowledge sharing (spanning disciplines — from reaching the technical to the legal and ethical communities) and deliberations in data governance corresponds to one of these key building blocks.

Multi-stakeholder discussions and public-private partnerships will be critical to the development, adoption and implementation of data governance solutions for responsible AI in the military domain. The issue of data and its use in AI systems is one that encompasses both the public and private sectors; therefore, both sides of the spectrum will need to work together. As such, a clear distribution of roles and responsibilities between the different actors and across the life cycle of the technologies would therefore also be beneficial. As public and private actors reflect on their role and respective mandates in the wider AI policy landscape, they must acknowledge that states ultimately maintain certain sovereign prerogatives that are exclusive to them, while the private sector and civil society organizations maintain a level of flexibility and agility that states may not always have (Afina 2023). It is, however, important to note that how these actors interact, the level of interdependencies

32 See, for example, Winter and Davidson (2019).

33 The UNIDIR's RAISE is one example of such initiatives. In partnership with Microsoft, RAISE brings together track-two voices across sectors and across geopolitical divides to issue policy recommendations and implement governance solutions. Members include, but are not limited to, representatives from industry, the research community, civil society organizations, academia and international organizations from China, Ecuador, France, India, Mauritius, Namibia, Poland, Russia, the United Kingdom and the United States.

and the potential hierarchies vary, often to a great degree, depending on states' policies, legal traditions and other factors such as socio-cultural approaches. Acknowledging this varying landscape, the authors do not wish to suggest that one model works better than others, although more discussions as to how multi-stakeholder and cross-sectoral engagement can be done in an effective manner would indeed be useful. The following constitutes suggested roles and responsibilities that are neither restrictive nor mutually exclusive:

- International organizations can help provide a neutral, independent platform for the development and eventual adoption of high-level norms, principles and standards at the international level. Subject to their respective mandate, regional organizations can play a critical role in providing a more contextualized and adapted platform for more granular deliberations and the eventual development, adoption and implementation of norms and principles surrounding data governance. Both international and regional organizations can play a critical role, through collaboration, in building the capacity of state and non-state stakeholders with regard to fostering data practices to support responsible AI in the military domain.
- States would maintain their sovereign prerogative of norm setting and policy making and develop oversight and verification mechanisms to assist with the enforcement and implementation of policies and regulations. In this sense, it would be useful for each state to dissect the specific roles and responsibilities each agency can play. Armed forces can, for example, help translate policies, norms and regulations into rules of engagement, while regulators (for example, for privacy) and ministries of justice can, for example, shed clarity on the applicability and application of frameworks dedicated to civilian applications to the military domain (for example, the EU AI Act). In certain cases, such regulators and agencies may be at the supranational level (for example, within the European Union, this would be the European AI Office). Under all circumstances, cross-agency cooperation and coordination will be important, for which capacity will be key.
- Much, if not most, of today's technological innovation is driven and led by the private sector. In addition to the increasingly dual-use nature of many, if not most, technologies, both major industries and small and medium enterprises play a critical role in supporting governmental entities, including to inform with technical expertise and solutions; public-private partnerships will also be key in the execution and operationalization of many of the norms and principles for the responsible development, deployment and use of AI in the military domain.
- In light of AI's widespread deployment and the blurred lines between the civilian and military realms with regard to data practices, the effects and implications on civilians, and their perspectives, cannot be overlooked. Civil society organizations, due to their proximity to civilians, will play a critical role in maintaining public oversight on the development and implementation of governance solutions, and uphold human rights norms. In addition, civil society organizations play a critical role in aiding with the implementation and operationalization of norms directly, which will be critical, especially in times of conflict when civilians are most vulnerable.

This mapping will ultimately contribute to efforts to maintain levels of traceability over the data throughout its life cycle.[34] Key points of consideration to help establish the data's traceability include:

- Where does the data come from?
- Who has collected the data?
- Why did they collect the data?
- What are the methods and parameters used to collect the data?
- Has the data been processed in any way? If so, how, why and by whom?
- What data hygiene practices has the data gone through? By whom and how?
- How has the data been stored?
- Has the data been sold and, if so, under what terms and conditions has the transaction been agreed on and by whom?

34 The concept of data "traceability" is an approach that is increasingly explored, across disciplines, for quality assurance, for building trust and for maintaining accountability and responsibility over data practices. See, for example, Beckers et al. (2016), Lee (2019) and Olaya et al. (2023).

- Will the data be sold elsewhere and to other users?
- What jurisdiction(s) and, subsequently, laws and regulations apply to the data?
- Who holds ownership or intellectual property rights over the data?
- Has the data been used to train AI models? If so, how and why?

Yet, for public-private partnerships to work, there is a need for deeper reflections on how to ensure their effectiveness. There is also a need to further reflect on incentivization, which ultimately consists of a two-fold effort: one, how to incentivize non-state entities, that is, industries, civil society organizations and academia to partner and work with states toward implementing responsible data practices; and two, how to incentivize states to engage with, and involve, to a certain extent, non-state entities in governance efforts, cognizant of national realities, the local policy and economic context, laws and regulations.

Creation of Standards and Procedures

The implementation of standards and procedures is a means through which soft law, complementing hard laws and regulations, can ensure that governance practices are implementable and provide a pathway to ensuring good practice and compliance. Several avenues could be explored:

- Transparency standards and guidelines could be promoted with regard to the data and its transformation. This would serve to ensure that data, its parameters and assumptions are made available to the different actors involved in the life cycle of AI systems and its various elements. This could include transparency around why the data has been collected, where the data has come from, who has transformed it and how. It could also serve to provide standards or guidelines in terms of how to collect, transform, analyze and dispose of data.
- Agreements on data exchange practices would need to be put in place between the different entities involved across the life cycle of AI data. This would involve intragovernmental entities, including within the defence department or ministry and at the interministerial level, as well as external entities, namely, private companies. This would notably require guidance or standards as to what should be expected or agreed upon in service contracts between public and private entities. For example, ensuring that data does not become "locked in" with a particular entity or service. In addition, what these practices mean for existing cross-border data practices and frameworks, especially in the intelligence and law enforcement realms, will need to be further unpacked.
- Testing procedures, evaluation metrics and benchmarks could be established to improve data practices. For example, data, at different stages of its life cycle, could be subject to red-teaming or targeted review, to ensure that it meets the necessary standards. Sandboxing, or the testing in a secure, isolated environment, can also be a way of assessing different data sets, and could be established as a standard practice.
- Clear roles and responsibilities for those owning and involved and working closely with data, including AI data, are important to determine accountability and to ensure that there is compliance with data governance principles. At the national level, this could, for example, include the position of a chief AI data officer. Ideally, this position would be able to work closely with colleagues working on data and digital technologies in the defence department or ministry as well as across government. However, given that such sources can be shared or merged, including beyond national entities, there is also a question of how to ensure responsibility and ownership in cases where data is shared with and used by multiple states or data is shared with and used by non-state entities for military purposes (for example, private military companies or other non-state armed groups).

While the creation of standards is important, ensuring contextualization of standards and procedures is also crucial (Afina 2024). Beyond the need for international frameworks and standards, an application of regional and local contexts and nuances must also be taken into account. This can mirror ways in which certain disarmament frameworks have been set up, in that there is an overarching global framework, which is then applied regionally to ensure that the framework responds to issues that are most relevant to each region. In the case of data governance, regional and local contexts

should be taken into account and structural issues, such as differences in data availability, or data localization, should be considered.

Information Sharing

Information sharing can foster collaboration and cooperation, as well as being fostered by them. A platform through which best practices and relevant information surrounding data practices for AI in the military domain can be shared at various levels — including among the technical community and representatives at the policy level, as well as in track 1.5 and track two settings — could help achieve this. National sensitivities and regional contexts would need to be managed or at least factored in, but this type of exchange can be particularly useful in a context where there is limited expertise and the need to ensure capacity building. More generally, information sharing is a key pillar to confidence and trust building — and as such must be facilitated through neutral platforms (for example, within the UN ecosystem).

Information shared and lessons learned could, for example, encompass the following aspects:

- how to ensure that data governance principles are embedded in contracts with external suppliers;
- structures that have been created or would be necessary to uphold data governance; and
- research studies on the development of appropriate AI data governance policy instruments in the military domain.

Data Equity

As discussed above, responsible AI is currently at the core of many of the discussions on the use of AI in the military domain. Yet responsible AI should also be synonymous with responsible data practices. In this context, it is important to consider issues of data equity in terms of how data is collected and processed and, more generally, the data processes surrounding AI innovation and use. A salient example illustrating the importance of data equity is the data labelling outsourcing by OpenAI to help build ChatGPT. There have been reports that OpenAI contracted Kenyan workers to label harmful content, including content featuring sexual abuse, hate speech and violence. These tasks are key to enabling safe and secure use of ChatGPT, but the working conditions were precarious, and workers received little mental health support and were underpaid (Perrigo 2023). As studies on data equity — and the implications of rapid AI development and deployment — emerge, any efforts to promote responsible AI in the military domain ought to factor in equity considerations and consult closely with state and non-state stakeholders.[35]

Research Gaps

Several pathways for consideration and operationalization are discussed in the sections above but data governance for responsible AI remains, overall, severely under-researched and under-resourced. Specific research could be carried out on several key aspects, namely:

- The applicability and application of existing AI governance and data governance structures, such as the GDPR or EU AI Act, to AI data governance in the military domain: This research could focus on creating an overview of good practices that are applicable in the military domain, such as inclusion of a provision on data governance in procurement contracts, and specifics on the distribution of roles and responsibility. This research could also clarify the applicability of these laws and regulations on dual-use technologies, especially in the spirit of demystifying the absolute exclusion of military applications from these frameworks.
- Consideration of complementary technologies for data governance: Further studies would benefit this space as to how certain technologies leveraged in the civilian sphere, such as PETs, federated learning and blockchain technologies, can not only promote privacy in data trading processes but also be used as a means of tracing the source and transfer history of the traded data (Afina and Persi Paoli 2024).[36]
- Translation of ethical and legal considerations, such as accountability, transparency, explainability or corporate responsibility, into actionable technical requirements throughout the life cycle of data: This is particularly relevant to data collection and data hygiene. This should be achieved in conjunction with discussions on

35 See, for example, Stonier et al. (2023).

36 On PETs and federated learning, see, for example, Shteyn, Kollnig and Inverarity (2023) and Inverarity (2023).

responsible AI more broadly and is a topic for consideration by military legal advisers as well.

→ An exploration of the possible application pathways and impact military AI data governance could have on the efficiency and efficacy of military applications more generally, and military action in the context of a military operation: It would be relevant and timely to explore the differences in application of military AI governance in the context of non-combat military applications versus combat applications, and also whether and how data governance can be maintained in the context of a military operation where timeliness of action, a core imperative, may compete with the need to comply with AI data governance principles.

Conclusion

Data is at the core of AI. At the same time, as increasing amounts of data are collected through innumerable sensors and collection methods, AI is becoming essential to help make sense of these masses of "raw material." In this co-dependent relationship, poor-quality data will result in poor-quality outcomes — or "garbage in, garbage out." In the context of the military, given the breadth of areas where AI is and could be used, this could have a series of consequences, ranging from harmless to disastrous, depending on where AI is applied and to what end.

As such, ensuring the quality of the data is important — as is ensuring its access, understanding how it may have been transformed and being aware of the possible implications, namely, legal and ethical, of such data. This is of particular importance given the inherent dual-use nature of data used in the military domain, and the questions the use of such data pose with regard to civilian data governance but also international law, namely, IHL and IHRL.

In light of the benefits that AI could afford military organizations, it has become an increasingly central component referenced within military strategies, postures and national and regional security policies. Yet it is acknowledged that the misuse of such a technology, as well as its irresponsible development, deployment and use, could lead to (severely) harmful consequences. As such, multiple initiatives have sprung up with the aim of operationalizing responsible AI in the military domain, such as REAIM and the Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy led by the United States.

To date, discussions have been very focused on AI systems themselves, and the issues pervasive to these systems — such as predictability, understandability and explainability of AI. However, these discussions should be broadened and should include the question of data and its governance. Discussions on responsible AI should encompass those of "responsible AI data"; this element is essential to achieving responsible AI in the military domain more broadly. States should consider the importance of a multi-stakeholder dialogue, since both AI systems and, to an even greater extent, the data enabling these systems encompass a wide range of actors. Moreover, questions of responsible AI and governance of AI data are not restricted to the military domain; expanding these conversations and learning from what has been achieved in the wider security and defence context (for example, in the context of law enforcement, counter-piracy and counterterrorism efforts, border security, national security and surveillance), as well as cross-pollination with the civilian domain will provide a helpful foundation from which to build from to achieve responsible AI — one that takes into account all the elements that form and enable an AI system.

Works Cited

Abraham, Yuval. 2024. "'Lavender': The AI machine directing Israel's bombing spree in Gaza." *+972 Magazine*, April 3. www.972mag.com/lavender-ai-israeli-army-gaza/.

Afina, Yasmin. n.d. "International Humanitarian Law Considerations for the Development of AI-enabled Technologies for Military Targeting Operations." Ph.D. thesis (in progress).

———. 2023. "How to deal with military AI's Oppenheimer moment." The World Today, September 29. www.chathamhouse.org/publications/the-world-today/2023-10/how-deal-military-ais-oppenheimer-moment.

———. 2024. *The Global Kaleidoscope of Military AI Governance: Decoding the 2024 Regional Consultations on Responsible AI in the Military Domain*. September 5. Geneva, Switzerland: UNIDIR. https://unidir.org/publication/the-global-kaleidoscope-of-military-ai-governance/.

Afina, Yasmin and Giacomo Persi Paoli. 2024. "Governance of Artificial Intelligence in the Military Domain: A Multi-stakeholder Perspective on Priority Areas." Policy Brief. September 5. Geneva, Switzerland: UNIDIR. https://unidir.org/wp-content/uploads/2024/09/UNIDIR_Governance_of_Artificial_Intelligence_in_the_Military_Domain_A_Multi-stakeholder_Perspective_on_Priority_Areas.pdf.

Africa Defense Forum. 2023. "Nigerian Navy to Harness Artificial Intelligence to Strengthen Operations." Africa Defense Forum, October 24. https://adf-magazine.com/2023/10/nigerian-navy-to-harness-artificial-intelligence-to-strengthen-operations/.

AI Task Force. 2019. *Artificial Intelligence in Support of Defence*. Report of the AI Task Force. September. Paris, France: Ministère des Armées. www.defense.gouv.fr/sites/default/files/aid/Report%20of%20the%20AI%20Task%20Force%20September%202019.pdf.

Arab News. 2024. "WhatsApp being used to target Palestinians through Israel's Lavender AI system." Arab News, April 19. www.arabnews.com/node/2495816/media.

Batlle, Sergi and Arnaud van Waeyenberge. 2024. "EU-US Data Privacy Framework: A First Legal Assessment." *European Journal of Risk Regulation* 15 (1): 191–200. https://doi.org/10.1017/err.2023.67.

Beckers, Kristian, Jörg Landthaler, Florian Matthes, Alexander Pretschner and Bernhard Waltl. 2016. "Data Accountability in Socio-Technical Systems." In *Enterprise, Business-Process and Information Systems Modeling*, edited by R. Schmidt, W. Guédria, I. Bider and S. Guerreiro. Lecture Notes in Business Information Processing, vol. 248. Cham, Switzerland: Springer. https://doi.org/10.1007/978-3-319-39429-9_21.

Bhuiyan, Johana. 2022. "Ukraine uses facial recognition software to identify Russian soldiers killed in combat." *The Guardian*, March 24. www.theguardian.com/technology/2022/mar/24/ukraine-facial-recognition-identify-russian-soldiers.

Bode, Ingvild. 2024. "Falling under the radar: the problem of algorithmic bias and military applications of AI." *Humanitarian Law & Policy* (blog), March 14. https://blogs.icrc.org/law-and-policy/2024/03/14/falling-under-the-radar-the-problem-of-algorithmic-bias-and-military-applications-of-ai/.

Cabitza, Federico, Andrea Campagner and Clara Balsano. 2020. "Bridging the 'last mile' gap between AI implementation and operation: 'data awareness' that matters." *Annals of Translational Medicine* 8 (7). http://dx.doi.org/10.21037/atm.2020.03.63.

Chandler, Katherine. 2021. *Does Military AI Have Gender? Understanding Bias and Promoting Ethical Approaches in Military Applications of AI*. Geneva, Switzerland: UNIDIR. https://unidir.org/publication/does-military-ai-have-gender-understanding-bias-and-promoting-ethical-approaches-in-military-applications-of-ai/.

Chu, Dexter. 2024. "AI Data Governance." *Secoda Data Engineering Blog*, September 12. www.secoda.co/blog/ai-data-governance.

Cone, Edward and Kayla Luparello. 2023. "The race for data supremacy: Achieving decision advantage to deter future conflicts." Oxford Economics, September. www.oxfordeconomics.com/wp-content/uploads/2023/09/IBM-The-race-for-data-supremacy.pdf.

DataGuidance by OneTrust and Baptista Luz Advogados. 2024. "Comparing privacy laws: GDPR v. LGPD." https://ec.europa.eu/futurium/en/system/files/ged/dataguidance-gpdr-lgpd-for-print.pdf.

Dave, Paresh and Jeffrey Dastin. 2022. "Exclusive: Ukraine has started using Clearview AI's facial recognition during war." Reuters, March 15. www.reuters.com/technology/exclusive-ukraine-has-started-using-clearview-ais-facial-recognition-during-war-2022-03-13/.

Deeks, Ashley, Noam Lubell and Daragh Murray. 2019. "Machine Learning, Artificial Intelligence, and the Use of Force by States." *Journal of National Security Law & Policy* 10 (1): 1–25. https://jnslp.com/wp-content/uploads/2019/04/Machine_Learning_Artificial_Intelligence_2.pdf.

Deng, Harry. 2023. *Exploring Synthetic Data for Artificial Intelligence and Autonomous Systems: A Primer*. Geneva, Switzerland: UNIDIR. https://unidir.org/wp-content/uploads/2023/11/UNIDIR_Exploring_Synthetic_Data_for_Artificial_Intelligence_and_Autonomous_Systems_A_Primer.pdf.

Department of Defense. 2023. *Data, Analytics, and Artificial Intelligence Adoption Strategy: Accelerating Decision Advantage*. June 27. https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF.

Department for Science, Innovation & Technology. 2023. "Safety and security risks of generative artificial intelligence to 2025 (Annex B)." GOV.UK, October 25. www.gov.uk/government/publications/frontier-ai-capabilities-and-risks-discussion-paper/safety-and-security-risks-of-generative-artificial-intelligence-to-2025-annex-b.

Department of Defense (Netherlands). 2023. *Defense Strategy Data Science and AI 2023–2027*. www.rijksoverheid.nl/documenten/rapporten/2023/05/31/defensie-strategie-data-science-en-artificiele-intelligentie-2023-2027.

Desjardins, Jeff. 2019. "How much data is generated each day?" World Economic Forum, April 17. www.weforum.org/agenda/2019/04/how-much-data-is-generated-each-day-cf4bddf29f/.

Ekelhof, Merel and Giacomo Persi Paoli. 2020. "The human element in decisions about the use of force." Geneva, Switzerland: UNIDIR. https://unidir.org/publication/human-element-decisions-about-use-force.

Electric Power Research Institute. 2020. "A Primer on Data Governance for a Responsible Artificial Intelligence in the Power Industry." January 15. www.epri.com/research/products/000000003002017792.

Eversden, Andrew. 2020. "Before joint all-domain operations, leaders need to solve data problems first." C4ISRNET, October 13. www.c4isrnet.com/show-reporter/ausa/2020/10/13/before-joint-all-domain-operations-leaders-need-to-solve-data-problems-first/.

Gerstein, Daniel M. and Erin N. Leidy. 2024. *Emerging Technology and Risk Analysis: Artificial Intelligence and Critical Infrastructure*. Homeland Security Operational Analysis Center. www.rand.org/content/dam/rand/pubs/research_reports/RRA2800/RRA2873-1/RAND_RRA2873-1.pdf.

Goldfarb, Avi and Jon R. Lindsay. 2022. "Prediction and Judgment: Why Artificial Intelligence Increases the Importance of Humans in War." *International Security* 46 (3): 7–50. https://direct.mit.edu/isec/article/46/3/7/109668/Prediction-and-Judgment-Why-Artificial.

Government of the Netherlands. 2023. "REAIM 2023 Call to Action." February 16. www.government.nl/documents/publications/2023/02/16/reaim-2023-call-to-action.

Grand-Clément, Sarah. 2023. *Artificial Intelligence Beyond Weapons: Application and Impact of AI in the Military Domain*. Geneva, Switzerland: UNIDIR. https://unidir.org/publication/artificial-intelligence-beyond-weapons-application-and-impact-of-ai-in-the-military-domain/.

Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons System. 2023. "Report of the 2023 session of the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems." CCW/GGE.1/2023/2, May 23. https://docs-library.unoda.org/Convention_on_Certain_Conventional_Weapons_-Group_of_Governmental_Experts_on_Lethal_Autonomous_Weapons_Systems_(2023)/CCW_GGE1_2023_CRP.2_12_May.pdf.

He, Alex. 2023. *State-Centric Data Governance in China*. CIGI Paper No. 282. Waterloo, ON: CIGI. www.cigionline.org/publications/state-centric-data-governance-in-china/.

Hern, Alex. 2022. "TechScape: Clearview AI was fined £7.5m for brazenly harvesting your data — does it care?" The Guardian TechScape Newsletter, May 25. https://theguardian.com/technology/2022/may/25/techscape-clearview-ai-facial-recognition-fine.

Holland Michel, Arthur. 2023. "Recalibrating assumptions on AI." Chatham House, April 12. www.chathamhouse.org/2023/04/recalibrating-assumptions-ai.

Houser, Kimberly A. and John W. Bagby. 2024. "Next-Generation Data Governance." *Duke Law & Technology Review* 21 (1): 61–106. https://scholarship.law.duke.edu/dltr/vol21/iss1/2.

ICRC. 2009. "Direct participation in hostilities: Questions & answers." February 6. www.icrc.org/en/article/direct-participation-hostilities-questions-answers.

Inverarity, Calum. 2023. "Modern PETs and confidential computing: no way out from GDPR obligations." *Open Data Institute Blog*, September 8. https://theodi.org/news-and-events/blog/modern-pets-and-confidential-computing-no-way-out-from-gdpr-obligations/.

Israel Defense Forces. 2024. "The IDF's Use of Data Technologies in Intelligence Processing." Press release, June 18. www.idf.il/en/mini-sites/idf-press-releases-israel-at-war/june-24-pr/the-idf-s-use-of-data-technologies-in-intelligence-processing/.

Kayser-Bril, Nicolas. 2020. "Google apologizes after its Vision AI produces racist results." AlgorithmWatch, April 7. https://algorithmwatch.org/en/google-vision-racism/.

Kilkenny, Monique F. and Kerin M. Robinson. 2018. "Data quality: 'Garbage in — garbage out.'" *Health Information Management Journal* 47 (3): 103–05. https://doi.org/10.1177/1833358318774357.

King, Anthony. 2024. "Digital Targeting: Artificial Intelligence, Data, and Military Intelligence." *Journal of Global Security Studies* 9 (2). https://doi.org/10.1093/jogss/ogae009.

Lee, Doyoung. 2019. "Big Data Quality Assurance Through Data Traceability: A Case Study of the National Standard Reference Data Program of Korea." *IEEE Access* 7: 36294–99. https://doi.org/10.1109/ACCESS.2019.2904286.

Lin-Greenberg, Erik. 2020. "Allies and Artificial Intelligence: Obstacles to Operations and Decision-Making." *Texas National Security Review* 3 (2): 56–76. http://dx.doi.org/10.26153/tsw/8866.

Liu, Fang and Demosthenes Panagiotakos. 2022. "Real-world data: a brief overview of the methods, applications, challenges and opportunities." *BMC Medical Research Methodology* 22. https://bmcmedresmethodol.biomedcentral.com/articles/10.1186/s12874-022-01768-6.

Meacham, Darian and Martin Gak. 2022. "Does facial recognition tech in Ukraine's war bring killer robots nearer?" openDemocracy, March 30. www.opendemocracy.net/en/technology-and-democracy/facial-recognition-ukraine-clearview-military-ai/.

Meerveld, H. W., R. H. A. Lindelauf, E. O. Postma and M. Postma. 2023. "The irresponsibility of not using AI in the military." *Ethics and Information Technology* 25 (14). https://doi.org/10.1007/s10676-023-09683-0.

Middle East Monitor. 2024. "Israel using Meta's WhatsApp to kill Palestinians in Gaza through AI system." Middle East Monitor, April 18. www.middleeastmonitor.com/20240418-israel-using-metas-whatsapp-to-kill-palestinians-in-gaza-through-ai-system/.

Ministry of Defence. 2021. *Data Strategy for Defence: Delivering the Defence Data Framework and exploiting the power of data.* Edition 1. September. London, UK: Ministry of Defence. https://assets.publishing.service.gov.uk/media/614deb7a8fa8f561075cae0b/Data_Strategy_for_Defence.pdf.

Nurkin, Tate and Julia Siegel. 2023. *Battlefield Applications for Human-Machine Teaming: Demonstrating Value, Experimenting with New Capabilities, and Accelerating Adoption.* August. Washington, DC: Atlantic Council. www.atlanticcouncil.org/in-depth-research-reports/report/how-modern-militaries-are-leveraging-ai/.

Olaya, Paula, Dominic Kennedy, Ricardo Llamas, Leobardo Valera, Rodrigo Vargas, Jay Lofstead and Michela Taufer. 2023. "Building Trust in Earth Science Findings through Data Traceability and Results Explainability." *IEEE Transactions on Parallel and Distributed Systems* 34 (2): 704–17. https://doi.org/10.1109/TPDS.2022.3220539.

Olejnik, Lukasz. 2022. "Smartphones Blur the Line Between Civilian and Combatant." *Wired*, June 6. www.wired.com/story/smartphones-ukraine-civilian-combatant/.

OneTrust DataGuidance. n.d. "Comparing privacy laws: GDPR v. Nigeria Data Protection Regulation." www.dataguidance.com/sites/default/files/gdpr_v._nigeria.pdf.

———. 2024. "Comparing privacy laws: GDPR v. PIPL." www.dataguidance.com/sites/default/files/gdpr_v_pipl_.pdf.

OneTrust DataGuidance, OneTrust DataGuidance Regulatory Research and Blumenthal Richter & Sumet. 2019. "Comparing privacy laws: GDPR v. Thai Personal Data Protection Act." www.dataguidance.com/sites/default/files/gdpr_v_thailand_updated.pdf.

Orso, Alessandro, Taweesup Apiwattanapong and Mary Jean Harrold. 2003. "Leveraging field data for impact analysis and regression testing." *ACM SIGSOFT Software Engineering Notes* 28 (5): 128–37. https://dl.acm.org/doi/abs/10.1145/949952.940089.

Perrigo, Billy. 2023. "Exclusive: OpenAI Used Kenyan Workers on Less Than $2 Per Hour to Make ChatGPT Less Toxic." *Time*, January 18. https://time.com/6247678/openai-chatgpt-kenya-workers/.

Puscas, Ioana. 2023. *AI and International Security: Understanding the Risks and Paving the Path for Confidence-Building Measures.* Geneva, Switzerland: UNIDIR. https://unidir.org/publication/ai-and-international-security-understanding-the-risks-and-paving-the-path-for-confidence-building-measures/.

Scharre, Paul. 2019. "Military Applications of Artificial Intelligence: Potential Risks to International Peace and Security." In *The Militarization of Artificial Intelligence*, 11–18. August. Stanley Center for Peace and Security, UN Office for Disarmament Affairs and Stimson Center. https://stanleycenter.org/publications/militarization-of-artificial-intelligence/.

Schenoni, Luis and Raul Madrid. 2024. "The Militarization of Latin American Security, Then and Now." Lawfare, April 28. www.lawfaremedia.org/article/the-militarization-of-latin-american-security-then-and-now.

Schraagen, Jan Maarten. 2023. "Responsible use of AI in military systems: prospects and challenges." *Ergonomics* 66 (11): 1719–29. https://doi.org/10.1080/00140139.2023.2278394.

Shah, Parth, Imani Thornton, Danielle Turrin and John E. Hipskind. 2023. "Informed Consent." In *StatPearls*. Treasure Island, FL: StatPearls. www.ncbi.nlm.nih.gov/books/NBK430827/.

Shteyn, Anastasia, Konrad Kollnig and Calum Inverarity. 2023. *Federated learning: an introduction*. Open Data Institute. January. https://theodi.org/insights/reports/federated-learning-an-introduction-report/.

Spencer, Sarah. 2024. "Humanitarian Aid?: Considerations for the Future of AI-use in Humanitarian Action." *Elrha* (blog), January 17. www.elrha.org/news-and-blogs/ai-use-in-humanitarian-action/.

Stonier, JoAnn, Lauren Woodman, Majet Alshammari, Renée Cummings, Nighat Dad, Arti Garg, Alberto Giovanni Busetto et al. 2023. "Data Equity: Foundational Concepts for Generative AI." *ArXiv*, October 27. https://arxiv.org/abs/2311.10741.

Svenmarck, Peter, Linus Luotsinen, Mattias Nilsson and Johan Schubert. 2018. "Possibilities and Challenges for Artificial Intelligence in Military Applications." NATO and STO.

The Department of National Defence and Canadian Armed Forces. 2019. *The Department of National Defence and Canadian Armed Forces Data Strategy*. Ottawa, ON: Government of Canada. www.canada.ca/content/dam/dnd-mdn/documents/reports/data-strategy/2019/dgm-25419-j4j-data-strategy-dia-en.pdf.

The White House. 2023. "Fact Sheet: President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence." Statements and releases, Octobwe 30. www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/.

The World Bank. 2021. "Data as a force for public good." In *World Development Report 2021: Data for Better Lives*. https://openknowledge.worldbank.org/bitstream/handle/10986/35218/9781464816000_Ch02.pdf.

UK Army. 2023. "British Army's Approach to Artificial Intelligence: A guide to accelerate the Army's adoption of AI and get the Army AI ready." October. www.army.mod.uk/media/24745/20231001-british_army_approach_to_artificial_intelligence.pdf.

United Nations. 2023. "Our Common Agenda Policy Brief 5: A Global Digital Compact — an Open, Free and Secure Digital Future for All." May. www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-gobal-digi-compact-en.pdf.

United Nations General Assembly. 2021. *The right to privacy in the digital age*. Report of the United Nations High Commissioner for Human Rights. A/HRC/48/31. September 15. www.ohchr.org/en/documents/thematic-reports/ahrc4831-right-privacy-digital-age-report-united-nations-high.

———. 2024. "Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development." A/78/L.49. https://undocs.org/A/78/L.49.

United Nations High-level Advisory Body on Artificial Intelligence. 2023. *Governing AI for Humanity*. Interim Report. December. www.un.org/techenvoy/sites/www.un.org.techenvoy/files/ai_advisory_body_interim_report.pdf.

United Nations Human Rights Committee. 2019. "General comment No. 36 on article 6: right to life." CCPR/C/GC/36. September 3. www.ohchr.org/en/calls-for-input/general-comment-no-36-article-6-right-life.

———. 2020. "General Comment No. 37 on Article 21 (Right of peaceful assembly)." CCPR/C/GC/37. September 17. www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-37-article-21-right-peaceful.

United Nations Interregional Crime and Justice Research Institute and Interpol. 2024. *Toolkit for Responsible AI Innovation in Law Enforcement: Principles for Responsible AI Innovation*. Revised February 2024. https://unicri.it/sites/default/files/2024-02/02_Principles_Resp_AI_Innovation_Feb24.pdf.

Wallace, David, Shane Reeves and Trent Powell. 2021. "Direct Participation in Hostilities in the Age of Cyber: Exploring the Fault Lines." *Harvard National Security Journal* 12. https://heinonline.org/HOL/LandingPage?handle=hein.journals/harvardnsj12&div=6&id=&page=.

Winter, Jenifer Sunrise and Elizabeth Davidson. 2019. "Governance of artificial intelligence and personal health information." *Digital Policy, Regulation and Governance* 21 (3): 280–90. https://doi.org/10.1108/DPRG-08-2018-0048.

Centre for International
Governance Innovation

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org