Cambridge Forum on AI: Law and Governance (2025), **1**, e44, 1–21
doi:10.1017/cfl.2025.10028

Cambridge Forum

RESEARCH ARTICLE

Architectures of AI: Tech power broking war?

Miah Hammond-Errey[1,2]

[1]Deakin University, Victoria, Australia and [2]Strat Futures Pty Limited, New South Wales, Australia
Email: miah@miahhe.com

(Received 20 January 2025; revised 22 June 2025; accepted 13 October 2025)

Abstract

This article investigates the profound impact of artificial intelligence (AI) and big data on political and military deliberations concerning the decision to wage war. By conceptualising AI as part of a broader, interconnected technology ecosystem – encompassing data, connectivity, energy, compute capacity and workforce – the article introduces the notion of "architectures of AI" to describe the underlying infrastructure shaping contemporary security and sovereignty. It demonstrates how these architectures concentrate power within a select number of technology companies, which increasingly function as national security actors capable of influencing state decisions on the resort to force. The article identifies three critical factors that collectively alter the calculus of war: (i) the concentration of power across the architectures of AI, (ii) the diffusion of national security decision making, and (iii) the role of AI in shaping public opinion. It argues that, as technology companies amass unprecedented control over digital infrastructure and information flows, most nation states – particularly smaller or less technologically advanced ones – experience diminished autonomy in decisions to use force. The article specifically examines how technology companies can coerce, influence or incentivise the resort-to-force decision making of smaller states, thereby challenging traditional notions of state sovereignty and international security.

Keywords: National security; intelligence; AI; security; war; resort-to-force

1. Introduction

Technology companies have emerged as powerful actors in the calculus of war and peace, as artificial intelligence (AI) systems are increasingly influencing state-level decision making on the resort to force (Erskine & Miller, 2024). The evolving literature on society-technology interactions has introduced concepts such as technology ecosystems, platforms, and stacks, which can help us to better understand the impact of AI on resort-to-force decision making. This article synthesises these concepts under the umbrella of "architectures of AI," focusing on the growing influence and power of technology companies – now largely synonymous with AI firms – in military decision making and state deliberations over the use of force. These firms form an "infrastructural core" (van Dijck, Poell & de Waal, 2018), which controls global information flows and services, thereby diminishing the capacity of nation states to make independent decisions on matters of war and peace.

This is one of fourteen articles published as part of the *Cambridge Forum on AI: Law and Governance* Special Issue, *AI and the Decision to Go to War*, guest edited by Toni Erskine and Steven E. Miller. Thank you to the reviewers for their extensive engagement and recommendations. Thank you to Toni, Steven and the team for your incredible support and convening this wonderful group.

© The Author(s), 2026. Published by Cambridge University Press. This is an Open Access article, distributed under the terms of the Creative Commons Attribution licence (http://creativecommons.org/licenses/by/4.0), which permits unrestricted re-use, distribution and reproduction, provided the original article is properly cited.

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

As Erskine (2024, p. 175) argues, the pervasive nature of AI suggests that "AI-driven systems will … increasingly influence the … consequential step of determining if and when a state engages in organised violence. In short, AI will infiltrate the decision to wage war". To date, power has been accumulated across each of the "architectures of AI." This article considers possibilities for how companies may wield that power in society and in relation to resort-to-force decision making. This article shows how technology companies are not merely providers but have become de facto national security actors, capable of impacting state sovereignty through direct coercion, indirect influence, or the strategic offering of incentives. Specifically, it sets out how US technology companies have an increasing capacity to coerce, influence or incentivise the decisions of smaller nation states, including in resort-to-force decision making.

This article contends that the accumulation and exercise of power within the architectures of AI are fundamentally altering the political calculus and practical realities of going to war. Specifically, it examines three interrelated dimensions: (i) the concentration of power in technology and digital infrastructure, (ii) the diffusion of national security decision making, and (iii) the role of AI in shaping public opinion. Taken together, these factors degrade the autonomy of nation states, particularly smaller or technologically reliant ones, in making sovereign resort-to-force decisions. While the analysis is grounded in an Australian perspective, its implications are relevant to liberal democracies globally.

2. The "architectures of AI": looking across the stack

This section outlines the often colloquially used term "tech (technology) stack" as well as the infrastructure underlying and essential for AI systems. I refer to these collectively as the "architectures of AI." Considering these components as architectures across the technology stack enables examination of actors (including companies and individuals) who are involved in AI. It also allows exploration of how changes to underlying infrastructures, architectures and applications of AI shape resort-to-force and national security decisions.

Academics and pioneers in the field define AI in different ways (Collins, Dennehy, Conboy & Mikalef, 2021). Different definitions have also been given to guide the research and development of AI policy and regulations. Moreover, AI definitions evolve over time. Early definitions tended to include comparisons to human intelligence, whereas more recent definitions tend to focus more specifically on AI's autonomy and goal-directed behaviour, as well as the acknowledgement of specific capabilities, including perception, reasoning, learning and problem-solving (Whelan, Hammond-Errey & Villeneuve-Dubuc, 2024). This article invokes the Australian Department of Industry, Science and Resources (DISR) definition of AI as "an engineered system that generates predictive outputs such as content, forecasts, recommendations, or decisions for a given set of human-defined objectives or parameters without explicit programming" (DISR, 2024). The DISR definition of AI is also based on the respective International Organization for Standardization (ISO) definition (ISO/IEC 22,989:2022).[1] The technical definitions of AI are important because they are clearer and more precise than general and popular references to a variety of technologies.

We can also think about AI, machine learning, and algorithms in the context of a "tech stack." The term "technology stack" or "tech stack" (also sometimes an "AI stack") is often used to describe the layers or levels of technologies, tools and software that companies use to build and maintain their digital products and services (Tsaih, Chang, Hsu & Yen, 2023). It is referred to as a stack to help visualise the technologies being stacked on top of each other, from frontend to backend, to build an

[1]The ISO develops and publishes international standards. These definitions were built on in subsequent ISO standards published in 2023, which include guidance on AI management systems (ISO/IEC 42,001:2023) and AI risk management (ISO/IEC 23,894:2023). This definition also includes the interrelated definitions of "machine learning" and "algorithm."

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

application. A stack can have many possible layers depending on the service or product. The AI tech-stack model is a conceptual framework[2] – it does not map onto specific systems (Tsaih et al., 2023) – but it does provide a lens through which to look at different layers of AI.

This article employs the term "technology companies" to refer to the entities driving contemporary AI development. In the current paradigm, AI and Big Tech are synonymous (Kak et al., 2023). Almost exclusively, AI development is dependent on these firms. This includes the compute capacity, data holdings and market reach to scale and sell AI products. (Kak et al., 2023). The distinction between "AI companies" and technology companies has thus largely dissolved, as the latter dominate the development and commercialisation of AI. Even ostensibly independent organisations, such as OpenAI, operate in close partnership with these firms (for example, with Microsoft). For these reasons, this article uses the broader term "technology companies" rather than "AI companies."

This article considers the underlying infrastructure – or architecture – essential for AI: data, energy generation and access, compute capacity, connectivity and workforce. I refer to these collectively as the "architectures of AI." The design of technology shows us where the power lies (Donovan, 2019), and the lens of architecture highlights how technology companies are entangled with politics and how they influence resort-to-force decision making. Understanding the architectures of AI allows us to observe accumulated power, consider the broader impact that technology companies have on policy and decision making, and identify how technology companies and government are enmeshed. Indeed, Rogers and Bienvenue (2021) argue that the layers of the technology stack act as gateways to accommodate influential gatekeepers who exert power over the flow of information across the stack.

3. Resort-to-force decision making and the architectures of AI

This article sets out how the architectures of AI have the capacity to influence nation-state deliberations on the resort to force. Thus, it is necessary to consider how such deliberations occur. This section provides a brief overview of the literature on technology, geopolitics, and resort-to-force decision-making. The empirical analysis regarding how such deliberations are made remains a complex and, in many respects, under-documented area of research. There is a substantial body of scholarship on the doctrinal and normative frameworks governing the use of force, such as legal and theoretical analyses in international law journals.[3] However, empirical studies that systematically examine the actual decision-making processes are comparatively scarce.

In international relations and law, much of the existing analysis focuses on the interplay between legal standards, risk assessment and other considerations, rather than on the empirical realities of how decisions to resort to force are made in practice. "States must make a variety of calculations when confronted with a decision about whether to use force against or inside another state. In use of force decisions, the divide between policy and legal doctrine is often disputed" (Deeks, Lubell & Murray, 2019, p. 3). International law is itself indifferent towards domestic political or constitutional prerequisites to using force (Hendell, 2023).[4] The literature on resort-to-force deliberations, whether about inputs or actual decision-making processes, is surprisingly slim outside the US. Existing works, largely focus on historical case studies, primarily in the US, nevertheless provide helpful insights. For example, Whitlark (2021), writing in the context of nuclear force, concludes that executive perspective and individual personality – not institutional structure – are paramount to such resort-to-force deliberations.

[2]The concept of a tech stack has also been applied in the design of political geography to make the fundamental claim that the stack is planetary-scale computation making system, replacing other forms of governance and sovereignty – with great political consequence (Bratton, 2015).

[3]See for example (Waxman, 2013; Bode, 2023).

[4]Perhaps this is because international law treats states as equal and therefore does not concern itself with their internal political machinations.

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

Increasing attention has been afforded to how private corporations play a powerful role in geopolitical decision making. For instance, Sommer, Matania and Hassid (2023) write, "the digital frontier of nations changed, and with it the concept of national security." They argue that there can no longer be an exclusive focus on territory and people. The concept of national security (like sovereignty and jurisdiction) is now heavily intertwined with tech companies and AI success.[5] To escalate an issue to a matter of national security is inherently a political choice. National security is also a matter of prudential value: a condition which must be maintained against others' potential to degrade it (Gyngell & Wesley, 2007).

Neilsen and Pontbriand (2025) consider how cyberattacks against privately owned and operated civilian critical infrastructure challenge the notion (so fundamental to liberal democracies) that war is premised on a strict delineation between military and civil domains. Their focus is on how NATO members understand their role in protecting civilian critical infrastructure. This article provides an excellent foundation for understanding the relationship between private and public in individual infrastructure and cybersecurity. However, it is less helpful for understanding power asymmetries and the impact of companies or individuals attempting to leverage the nation state and governing functions.

Less has been said about how AI powerbroking cultivates a climate in which private corporations have the capacity to influence, coerce or incentivise resort-to-force decision making by nation states. Kelton et al. (2022) suggest that US digital platforms, as exclusive service providers, seem to acquire some of the extractive and transformative power traditionally ascribed to the sovereign state and, moreover, sit beyond the sovereign state's capacity to regulate and control. Rogers and Bienvenue (2021, p. 96) argue that the layers of the technology stack act as gateways accommodating influential gatekeepers who exert power across it. In previous work, I have showed that the big data landscape, which includes AI, "will continue to alter national security by changing who has information and power to change and influence aspects of society" (Hammond-Errey, 2024, p. 182).

Schaake (2024b np) writes, "the involvement of Big Tech companies in active military conflicts raises tough questions about the concept that underpins the foundations of international relations and international law: state sovereignty." Schaake (2024b) notes that companies including Google, Microsoft and SpaceX have few, if any, legal mandates according to international law as they are private actors. "Companies are playing an ever more critical role in this strange cyber dividing line between war and peace" (Schaake, 2024b). This role is often considered in the context of geopolitics and state legislation and international affairs, as set out below:

> Yet companies… exude sovereign power in new ways. They have monopolies on key insights and data analytics and make decisions about affairs that were once the exclusive domain of states, while these companies are not subject to comparable checks and balances. Moreover, companies that operate at a global scale often chafe against geographic borders. Even when governments want to exert control over such companies … they face a variety of constraints (Schaake, 2024b).

This article moves beyond observing that technology companies are involved in geopolitics and instead highlights how this intersects with AI and resort-to-force decision making. There is a growing body of literature that looks at the use of technologies and AI in intelligence, which of course influences resort-to-force decision making. Intelligence – "knowledge vital for national survival" (Kent, 1966, p. vii) – forms an important input into resort-to-force deliberations. The impact of big data and

[5]One example is the 21 February 2025 Executive Order the White House released, titled *Recent Defending American Companies and Innovators From Overseas Extortion and Unfair Fines and Penalties The White House*. It has largely been seen as threatening retaliatory tariffs against countries trying to hold US technology companies accountable and ensure they pay their fair share of corporate taxes.

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

AI on national security and intelligence production plays a significant role in framing and deliberating on national security matters (Hammond-Errey, 2024). Hershkovitz (2022) and Zegart (2022) outline the transformative nature of AI to the practice of intelligence and its input into resort-to-force decision making.

Krasner (1999) makes the argument that the key attributes of sovereignty are never perfectly present. "There has never been some ideal time during which all, or even most, political entities conformed with all of the characteristics that have been associated with sovereignty – territory, control, recognition, and autonomy" (Krasner, 1999, p. 235). Alternative principles, such as human rights, fiscal responsibility and international security have been used to challenge autonomy. Krasnow (Krasner, 1999, p. 236) notes how "in the absence of any well-established hierarchical structure of authority, coercion and imposition are always options that the strong can deploy against the weak."

Indeed, the term "technology sovereignty" has emerged as a consequence of the power of technology companies. Edler, Blind, Kroll and Schubert (2023, p. 1) argue that "technology sovereignty should be conceived as a state-level agency within the international system, i.e., as sovereignty *of* governmental action, rather than (territorial) sovereignty *over* something." In the context of the architectures of AI, the impact of the sovereignty *of* governmental action includes deliberation processes on the resort to force. This includes deliberation on the role of (and access to) largely civilian digital infrastructure in conflict, especially if owned and/or operated by a foreign state. It also includes deliberation on ensuring access to civilian and military technology as well as underlying technological infrastructure such as connectivity, energy generation and access, compute capacity, and components such as advanced semiconductors.

This article argues that technology companies are national security actors and could use AI to influence resort-to-force decision making. Contemporary power is exercised in and through the architectures of AI. Companies that have monopolised the big data landscape of data abundance, digital connectivity and ubiquitous technology (Hammond-Errey, 2024) have centralised economic power and attained near-sovereign state-like status (Schaake, 2024a, 2024b; Khanal et al., 2024). Coupled with the inextricable reliance that governments have on these companies and technologies, the unprecedented scope and concentration of power in technology companies means that most nation states have, or will have, less autonomy in resort-to-force decisions. This could occur directly through coercion, indirectly as influence, or through incentivisation at any point, such as during the development of capabilities, pressure during conflict, through revocation of services, or even supporting potential adversaries. These will be explored throughout this article.

4. Architectures of AI: implications of concentration of power, diffused decision making and public opinion

This section considers the concentration of power across architectures of AI, data, energy generation and access, compute capacity, connectivity and workforce. It then explores areas of influence in resort-to-force deliberations across three important areas of focus: the concentration of power, the diffusion of national security decision making, and the role of AI and the information environment in shaping public support. The section reveals that because of the scope and concentration of power in technology companies, most nation states have, or will have, less autonomy in resort-to-force decisions, either directly through coercion, indirectly as influence or through incentives.

Digital infrastructure is the backbone of our societies. The technology ecosystem is dominated by a small number of companies across all levels of the architectures of AI. This concentrates information flows, critical data sets, computing power, and technical capabilities (Andrejevic, 2013; Cohen, 2017; Edward, 2020; Moore, 2016; van Dijck et al., 2018) that are essential for functioning democracies (Richmond, 2019; Watts, 2020). The dominance of these companies has handed them scale and influence akin to nation states (Lehdonvirta, 2022, p. 3), challenging the primacy of governments (Eichensehr, 2019). This, in turn, is transforming the relationships that companies have with nation

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

states, challenging conceptions of national security and ultimately (knowingly or unknowingly) influencing state decisions on the resort to force. This section first outlines the accumulation of power across the architectures of AI. It then considers diffused decision making. It subsequently explores the implications of this power concentration on resort-to-force decision making, either directly through coercion, indirectly as influence or through incentivisation. Finally, it outlines how AI has the capacity to shape public opinion, impacting, if not diminishing, state capacity to engage with its citizens.

4.1. Data

Data is the foundation of AI. The technology ecosystem has been dominated by a small number of companies, concentrating information flows, critical data sets and technical capabilities for analysis (Andrejevic, 2013; Cohen, 2017; Edward, 2020; Moore, 2016; van Dijck et al., 2018). The "epicenter of the information ecosystem that dominates North American and European online space is owned and operated by five high-tech companies, Alphabet-Google, Facebook, Apple, Amazon, and Microsoft" (van Dijck et al., 2018, p. 6). These companies have monopolised aspects of the big data landscape of data abundance, digital connectivity and ubiquitous technology (Hammond-Errey, 2024).

The constellation of technologies that constitute AI (Bell, 2018) require massive amounts of data. The companies that dominate the consumer-driven big data economy and own most of the data in the West include Alphabet (Google), Facebook, Amazon (Moore & Tambini, 2021; Neef, 2014; Sadowski, 2020; Zuboff, 2019), Microsoft (Moore & Tambini, 2021; Neef, 2014; Zuboff, 2019), Apple, Alibaba (Verdegem, 2022), Twitter/X (Neef, 2014), Uber (Neef, 2014; Sadowski, 2020), TikTok and Tencent (Verdegem, 2022). The vast majority of digital data is sold and resold for profit (Kitchin, 2014; Sadowski, 2020; Zuboff, 2019). Data and the ability to analyse it give substantial market power only to the largest online platforms Santesteban and Longpre (2020).

4.2. Compute capacity

Ownership of data storage and computational capacity is highly concentrated. It is estimated that Amazon, Microsoft, and Google together hold 70 percent of the global cloud infrastructure market, which includes the market for graphics processing unit (GPU) compute used in AI research (Lehdonvirta, 2023). "There are only a few companies that own exponential computing power, can attract AI talent, and have access to data to develop and train advanced machine/deep learning models" (Verdegem, 2021). Moreover, the computational capacity that these platforms rely on is geographically concentrated (Ghahramani, 2023). The US and China have the most public GPU clusters in the world. China leads in the number of GPU-enabled regions overall; however, the most advanced GPUs are highly concentrated in the US. The US has eight "regions" where H100 GPUs – the kind that are the subject of US government sanctions on China – are available to hire (Perrigo, 2024). In 2021, the US held a dominant pole position with 33 percent of global data centres, and the broader Organization for Economic Co-operation and Development (OECD) housed 77 percent of data centres (Daigle, 2021).

A similar story can be told with high-performance computers. As of June 2024, the first three and five of the top 10 most powerful non-distributed computer systems in the world are based in the US (Top500 2024, 2024). Additionally, across the top 500, the US accounts for 34.2 percent of the system total and 53.7 percent of the performance total (Top500 2024, 2024). Australia reportedly had 0.88 percent of the world's computing capacity as of November 2022, and the United Kingdom 1.3 percent – while the top five countries (the United States, Japan, China, Finland and Italy) had 79.1 percent (Top500, 2022). Lehdonvirta, Wu and Hawkins (2024, np) observe a global compute divide, in which "the geography of AI compute seems to be reproducing familiar patterns of global inequality."

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

The future of compute capacity is likely to continue to be geographically concentrated (Ghahramani, 2023).

4.3. Connectivity and infrastructure

The infrastructure of AI is predominantly owned by commercial entities, meaning that the data – and the ability to derive insights from it – largely resides in the private sector. Much of it is commercially available for purchase, and the analytical capabilities of big data have largely been built by – and reside in – industry (Crain, 2016; Kitchin, 2014). Despite offering a variety of different services (Lotz, 2018), a small handful of commercial entities have most of the world's data, information flows (Moore & Tambini, 2021; Neef, 2014; Omand & Phythian, 2018, p. 145; Zuboff, 2019), and computing capacity (Lehdonvirta, 2023; Verdegem, 2022).

Alphabet-Google, Facebook, Apple, Amazon, and Microsoft are therefore able to control the node of global information services (van Dijck et al., 2018). These companies do so in a way that was previously limited to telecommunications companies – assets that were historically government owned (Howell & Potgieter, 2020). Most internet users – nation state governments included – are dependent on these companies for their infrastructural information services (Cohen, 2017; Moore, 2016; van Dijck et al., 2018), including for computing (Lehdonvirta, 2023). This can be seen in the context of AI development specifically:

> In the context of the current paradigm of building larger- and larger-scale AI systems, there is no AI without Big Tech. With vanishingly few exceptions, every startup, new entrant, and even AI research lab is dependent on these firms. All rely on the computing infrastructure of Microsoft, Amazon, and Google to train their systems, and on those same firms' vast consumer market reach to deploy and sell their AI products (Kak et al., 2023).

Telecommunications infrastructure and undersea cables, which carry up to 99 percent of global internet traffic (Kelton et al., 2022), are critical to AI. Over the past decade, there has been a shift towards subsea cables built by large individual technology companies. Meta recently announced Project Waterworth, which plans to connect the US, India, South Africa, Brazil, Australia and other regions via a 50,000 km (31,000-mile) cable system. In addition, Big Tech companies have ownership of most cloud infrastructure and are involved in projects from low Earth orbit satellites to laser data transmission (Kelton et al., 2022). This challenges digital sovereignty in three ways, by impacting the ability of a country to control its technological infrastructure, its data (data security), and ability to provide internet-reliant services (Ganz, Camellini & Hine et al., 2024).

4.4. Energy generation and access

Since 2024, the role of tech companies in global energy generation and access has been elevated to a national security issue. While there is limited scholarship to date, policy and public discussion identify energy generation and access as key for AI. To state the obvious, "there is no AI without energy" (IEA [International Energy Agency], 2025). Leaders at COP29 debated the challenge of curbing AI emissions and domestically in the US, an increasing focus on the intersection between AI and energy, generation and access. For example, a September 2024 White House Roundtable considering the role of energy in AI Infrastructure[6] and October 2024 Memorandum on AI.[7] On 23 May 2025, the White House released an Executive Order that, among other things, designated AI data centres as "critical

[6]September 2024 *White House Roundtable on U.S. Leadership in AI Infrastructure.*

[7]On 12 Sep 2024, Readout of White House Roundtable on U.S. Leadership in AI Infrastructure https://www.whitehouse.gov/briefing-room/statements-releases/2024/09/12/readout-of-white-house-roundtable-on-u-s-leadership-in-ai-infrastructure/ and on 24 Oct 2024, Memorandum on Advancing the United States' Leadership in Artificial Intelligence; Harnessing Artificial Intelligence to Fulfil National Security Objectives; and Fostering the Safety, Security, and Trustworthiness of Artificial

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

defence facilities" and the nuclear reactors powering them as "defence critical electric infrastructure." It also mandates the rapid deployment of advanced nuclear technology to power AI infrastructure.[8] In July 2025, America's AI Action plan was released, which directly linked AI infrastructure and the energy to power it, noting "AI is the first digital service in modern life that challenges America to build vastly greater energy generation than we have today" (White House, 2025 p. 14).[9]

4.5. Workforce

The technology workforce for AI and its underlying architectures is an area of emerging scholarly interest. "There are only a few companies that own exponential computing power, can attract AI talent, and have access to data to develop and train advanced machine/deep learning models" (Verdegem, 2021). The impact of the AI workforce component, or "tech talent" as it is sometimes referred to, is increasingly considered within policymaking circles. For example, as part of the 2023 Quad Tech Network meeting, Koslosky (2023) explored the domestic and global shortages of the science, technology, engineering, and mathematics (STEM) workforce necessary for AI. While maintaining a STEM workforce is critical, it is an often-overlooked component of strengthening national critical technologies capabilities (Hammond-Errey, 2023). Moreover, as Assaad and Hammond-Errey (forthcoming 2025) note, "there is limited diversity in employer options for those with the skill sets to work on AI. This means knowledge around AI systems becomes siloed and sparse." Artifical intelligence researchers revealed the power, influence and dominance of the technology companies in AI research with limited public interest alternatives (Ahmed, Wahed & Thompson 2023)

4.6. Economic power

Economic power is a result of the concentration of power across the architectures of AI listed above. Economic power will be covered only briefly here due to the scope of this article; however, it is a topic of increasing scholarly and policy interest. The top five American technology companies (Alphabet-Google, Apple, Meta, Amazon, and Microsoft) have also amassed unprecedented economic power (Lee, 2021; Moore, 2016; Fernandez et al., 2021; Santesteban & Longpre, 2020). They had cumulative revenues of US$1.1 trillion in 2022, although their market capitalisation has dropped from a high of US$9.5 trillion in 2021 to US$7.7 trillion in April 2023 (Lee, 2021; Wall Street Journal, 2023abcde). Their combined market capitalisation in 2021 was more than six times the size of Australia's gross domestic product (GDP; US$1.55 trillion), while their revenues were almost twice the total revenue of the Australian governments (US$586 billion) in the same year (Australian Bureau of Statistics, 2023; World Bank, 2023). The market for military AI is lucrative and growing and, in the US alone, is projected to increase to 38.8 billion USD by 2028 (Schwarz, 2024).

Stucke and Grunes (2016) set out a range of factors needed to assess digital platform economic power, which include considerations relating to data, algorithms, network economies, economies of scale and scope, coordination, limiting competition and data transferability. The value of goods that passed through Amazon in 2022 (US$514 billion) exceeded the GDP of many countries – its 2021 revenue figure would place it in the top 30 countries for GDP (Amazon, 2023, p. 23; World Bank, 2023). Amazon's merchant fees in 2022 brought in more revenue (US$117 billion) than most states do through taxation (Lehdonvirta, 2022, p. 3). In some cases, these companies have taken on key functions akin to the judicial systems of nation-states – eBay rules on more financial disputes

Intelligence, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/10/24/memorandum-on-advancing-the-united-states-leadership-in-artificial-intelligence-harnessing-artificial-intelligence-to-fulfill-national-security-objectives-and-fostering-the-safety-security/. An outline of the implications for security can be seen here: https://www.lowyinstitute.org/the-interpreter/where-harris-trump-agree-ai-beat-china.

[8]23 May 2025, White House https://www.whitehouse.gov/fact-sheets/2025/05/fact-sheet-president-donald-j-trump-deploys-advanced-nuclear-reactor-technologies-for-national-security-f872/

[9]https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

(60 million) per year than any courts outside the United States hear on an annual basis (Lehdonvirta, 2022, p. 3).

4.7. Technology companies have accumulated power and governments are critically dependent

Technology companies are central to functioning democratic societies. In addition to the concentration of power outlined above, nation-state governments are critically dependent on Big Tech for the provision of government services. It is in the domain of US state and Big Tech relations that the consequences of the power concentration are already being felt. "Big Tech has become omnipresent and omnipotent in the policy process" (Khanal et al., 2024, p. 12). Their influence and resources result in semi-autonomous and semi-sovereign entities. States are also beginning to treat Big Tech like sovereign actors (Khanal et al., 2024). The immense power of technology companies can be seen in the geopolitical implications of their choices.

A wide range of companies are at the forefront of many national security threats, from data security and cyber security to telecommunications and critical infrastructure. Many of Australia's government agencies are heavily reliant on digital and technology services from the dominant players, ranging from the provision of data cloud services, email and office systems to AI application trials. In July 2024, the Australian Government and Amazon announced an AU$2 billion partnership to build a data cloud to store classified Australian military and intelligence information. This will see secure data centres built in secret locations across the country to support the purpose-built Top-Secret Cloud, which will be run by a local subsidiary of Amazon Web Services (Greene, 2024).

Decision making about national security continues in government. However, it also increasingly occurs in the private sector and especially within technology companies. Many of these decisions are consequential. As the Australian Privacy Commissioner Carly Kind said, "the major platforms are shaping society, they are not intermediaries" (Kind, 2024). This creates new dynamics regarding commercial decisions within companies as well as between government agencies, policymakers, and private-sector companies. These dynamics – and the competing tensions and complexities – are playing out in contemporary global conflicts.

This concentration of power presents new challenges, strategic and operational, to state resort-to-force decision making. This article shows that the concentration of power across the architectures of AI is indisputable and unlike any of the challenges to state sovereignty envisioned by Krasner (1999). The relationship between the US nation state and US-based technology companies is changing. Key technology actors are actively shaping the second Trump administration's technology posture and relationship to technology. Military and intelligence apparatuses cannot function without key technology companies. The latter control tools (among them, cloud systems or AI algorithms aimed at image and sound recognition, behaviour prediction and military targeting) are essential for surveilling adversaries (and "allies") and, if needed, to anticipate their moves on the battlefield (Coveri, Cozza & Guarascio, 2025; Gawer, 2022).

Increasingly, this accumulated power is intersecting with political and governance processes in the US. For example, Meta, Amazon, Google, Microsoft and Uber – as well as the CEOs of OpenAI and Apple – all made unprecedented tech donations of $1 million each to President-elect Donald Trump's inaugural fund (Harwell, 2025). These same companies advocated for the Executive Order *Removing Barriers to American Leadership in Artificial Intelligence* signed by President Trump on 23 January 2025. The order sees the dismantling of AI oversight and prioritises commercial dominance over collaborative global governance (Shafiabady & O'Neil, 2025). Four senior technology executives from Meta, OpenAI and Palantir were also sworn in as senior US Army officers (Nieberg, 2025). Another example of the role of Big Tech is Elon Musk's advisory role in the Trump administration and his position as a co-chair of a "government efficiency" panel, which resulted in an unprecedented concentration of power and conflicts of interest (Stone, 2024). X and Meta "are using this power in new ways

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

that declare war on facts, denigrate groups of people,[10] enhance vulnerabilities for state-sponsored interference,[11] influence foreign politics and decrease inclusion and participation" (Hammond-Errey, 2025). Musk has also used X to endorse and promote far-right political candidates – subsequently designated as extremists – in the United Kingdom and Germany (Kelly, 2025).

Contemporary power is accumulated in and through the architectures of AI. The architectures of AI are predominantly owned by technology companies, meaning that data and the ability to derive insights from it reside largely in the private sector or are available for purchase (Crain, 2016; Kitchin, 2014). This concentration of power pervades energy generation and access, as well as connectivity and workforce. It also combines with the existing concentration of economic power as well as policy and decision-making influence. Thus, in the not-so-distant future, it may well be impossible for nation state governments to operate their national infrastructure without service provision from AI technology companies. This leaves states open to companies influencing resort-to-force decision making, either directly through coercion or indirectly through forms of influence on policy processes and incentivisation.

5. The diffusion of national security decision making

The architectures of AI are hastening an existing trend: decision making about national security and decisions that impact national security continue within government but are also increasingly occurring outside government (Hammond-Errey, 2024). This section shows how the influence of decision makers in AI technology companies has diffused national decision making and created new national security actors. This, in turn, has impacted national security and decision-making processes, including on the resort to force. The architectures of AI are predominantly owned by commercial entities (the data – and the ability to derive insights from it – largely reside in the private sector or is available for purchase) (Crain, 2016; Kitchin, 2014). Technology companies are increasingly influencing government decision making, including on matters of war and security and are heavily involved in public policy and shaping policy processes (Khanal et al., 2024). Their influence and resources result in semi-autonomous and semi-sovereign entities. States are also beginning to treat Big Tech like sovereign actors (Khanal et al., 2024). These are all signs of nation states recognising the power technology companies have accumulated and foreshadow the potential they have to exercise it by influence, coercion, or incentivisation.

Cyberspace raises questions about who counts as a national security decision maker and how intelligence communities should interact with them (Zegart, 2022, p. 274). Further, companies create, use and control vast troves of personal data (Birch & Bronson, 2022), data storage and computational capabilities (Lehdonvirta, 2023), and information flows (Santesteban & Longpre, 2020). They have billions of users (Kemp, 2023) from whom they collect data and over whom they also have varying degrees of influence (Davidson, 2017; Griffin, 2019; Zuboff, 2019). Social reliance on digital infrastructure and providers of digital services means that many companies are a potential attack surface for national security threats in addition to being, increasingly, national security decision makers themselves (Hammond-Errey, 2024). Now, heads of companies – often in foreign countries – are national security actors. This adds a new dimension to decision making about war. For countries outside the US, this requires regulating technology and digital infrastructure while ameliorating citizen concerns about online harms and simultaneously considering government reliance on US technology companies. Technology companies have become important actors in modern conflicts, such as supporting Ukraine since the Russian invasion in February 2022 (Bresnick, Luong & Curlee, 2024).

The immense power of technology companies can be seen in the geopolitical implications of their choices. A wide range of companies are at the forefront of many national security threats, from data

[10] https://theintercept.com/2025/01/09/facebook-instagram-meta-hate-speech-content-moderation/

[11] https://www.lowyinstitute.org/the-interpreter/meta-s-decision-ditch-fact-checking-gives-state-sponsored-influence-operations-more

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

security and cyber security to telecommunications and critical infrastructure. Decision making about national security continues in government; however, it also increasingly occurs within technology companies. Many of these decisions are consequential. Coveri, Cozza & Guarascio (2025, p. 2) argue the interdependence between governments and technology companies… "challenges the traditional distinction between the state and the market, blurring their boundaries and, most importantly, questioning the willingness (and ability) of the former to control (and discipline) the latter in the collective interest." Furthermore, according to military scholars, key tech figures and companies are "hyping AI's role in war" (Lushenko & Carter, 2024). This creates new dynamics between commercial and national security decisions within companies as well as between government agencies, policymakers and private-sector companies. These dynamics – and the competing tensions and complexities – are playing out in contemporary global conflicts, even as the global order is changing.

Increasingly, technology companies are making specific choices about which services to provide to individuals and organisations at war. If a service, which an individual or company is reliant on, is provided or removed – or removal is threatened – it clearly operates as a form of coercion or influence. As one research report sets out, over the course of Russia's invasion of Ukraine, at least 18 privately held and publicly traded US technology companies offered services, often pro bono, in support of Kyiv's war effort (Bresnick et al., 2024). "These companies have provided support for communications and intelligence, reconnaissance, and surveillance (ISR) functions, delivered information that helped inform target selection, as well as protected Ukraine's critical infrastructure from cyberattack" (Bresnick et al., 2024, p. 6). In July 2024, the BBC reported that Microsoft shut down email and Skype accounts of Palestinians living outside Palestine and who tried to contact their families in Gaza (Shalaby & Tidy, 2024). In May 2025, after the US placed sanctions on the International Criminal Court's chief prosecutor, Karim Khan, Microsoft blocked his official email account (Quell, 2025). This has caused significant concern for policymakers around the world, including in Europe and Australia, due to the reliance on technology providers and their ability to influence or coerce nation state access to technology and limit decision-making scope.

Throughout Russia's invasion of Ukraine, Starlink provided online connections for civilian and military coordination (Lerman & Zakrzewski, 2022). The system – initially co-funded by Western governments (predominantly for the service's terminals) and SpaceX (for the connection) (Lerman & Zakrzewski, 2022; Metz, 2022) – was delivered at the start of the war and continued throughout the conflict, although not without disruptions at key moments and significant concern about continuity (Giles, 2023). The high-profile and public reliance of the Ukrainian military and civilian infrastructure on private company services and essential digital infrastructure has exposed new vulnerabilities. SpaceX signed an ongoing contract with the Pentagon to supply Starlink in Ukraine (Capaccio, 2023) in a more traditional arrangement.

Microsoft, Amazon and Google have also provided a range of services to Ukraine, including cybersecurity, the migration of critical government data to the cloud and keeping Ukraine connected during the Russian invasion (Bergengruen, 2024). Ukraine's use of tools provided by companies like Palantir and Clearview also raises complicated questions about when and how invasive technology should be used in wartime, as well as how far privacy rights should extend (Bergengruen, 2024). Horowitz (2023, 2024) provides an excellent outline of some of the legal considerations related to technology companies providing digital services in situations of armed conflict, and particularly the relationship between critical infrastructure companies, cyber offensives and defensive action that all blend into the traditional role of the state.

The prominent public role of Elon Musk and Starlink technology provides insight into the significant ability of individuals and companies to impact and make national security decisions outside of the traditional national security apparatus of government. As Giles notes, "companies are providing capabilities that are vital to Ukraine's national survival because they choose to, not because they are beholden to any of the states involved in the conflict" (Giles, 2023). This is clearly a concern to the US establishment: a recent Georgetown Center for Security and Emerging Technology (CSET) report

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

outlines US technology companies' financial and operational entanglements in China and argues that such entanglements complicate their decision making in a potential Taiwan contingency (Bresnick et al., 2024).

The technology landscape is evolving much more quickly than academic literature can capture. Concentrated power across the architectures of AI is already playing out in different examples in conflict and policymaking globally, including Ukraine and Russia as well as Israel and Gaza. It is also impacting international institutions that adjudicate on global norms related to war, such as the International Criminal Court. Leading AI technology companies and their leaders are all-new actors in governing and decision making, including now in matters of war. They are unelected, largely unaccountable, and wield immense power to covertly influence, coerce or even compel states to act in accordance with their wishes. They are extremely powerful in each of the architectures of AI, and governments are deeply dependent on them. Together, the concentration of power across the architectures of AI and diffused national security decision making decrease the scope of state decision making, even in relation to the resort to force.

6. AI's role in public opinion: curation, influence and interference

The role of AI is considered here in the context of shaping public opinion on war. AI is increasingly used by online news providers to curate and prioritise information and news. The social media platforms used most in Australia (Facebook, Instagram, WhatsApp and YouTube) as well as search services, are owned and operated by the large technology companies (Meta and Google) that have concentrated power across the architectures of AI. The AI algorithms and internal policies and processes behind social media – and in particular content discovery, curation, and moderation – shape public opinion. The applications and platforms we use "form a significant part of our information environment and have the capacity to shape us, including what we see, the choices we are presented with, what we think others believe, and ultimately how we might view the world" (Hammond-Errey, 2024b).

The role of public support in winning wars and the notion that wars are fought in the mind is central to military doctrine in the West (Libicki, 1995; Herbert & Kerr, 2021). In contemporary Western scholarship on the topic of adversary threats, the evolution of the use of public information campaigns in warfare has given rise to notions of hybrid war and threats (Hoffman, 2007), asymmetric war (Thornton, 2015) and grey-zone warfare (Hoffman, 2016), as well as several related (and competing) constructions to explain these phenomena (Galeotti, 2016; Selhorst, 2016). From a Western perspective, information forms a part of a broader warfare strategy used mostly by nation states. States use information and communication technology in pursuit of a competitive advantage over an opponent. This is usually combined with other military activities and directed by military strategy. In other words, states use the power of information and, increasingly, of public information to influence and achieve strategic results (Hammond-Errey, 2017). Similarly, Janis Berzins (2014) argues that the Russian view of modern warfare is based on the idea that the main battlespace is in the mind. Information is the principal tool in this fight, creating a version of reality that suits political and military purposes at all levels of warfare (Berzins, 2014, p. 5).

The interplay between public opinion and resort-to-force decision making in democracies has been the subject of long-standing controversy (Tomz, Weeks & Yarhi-Milo, 2020). Nevertheless, public opinion is inextricably linked with war. "Because battle is a matter of politics, as well as combat, the battlefield is not the only place where information is important. Information helps to shape opinion: let's go to war; let's not go to war; let's escalate and win an existing war; let's disengage from that war" (Seib, 2021, pp. 185–186). Arguably, contemporary wars are more about control of the population and the political decision-making process than about control over territory (Nissen, 2015). Thus, information dominance, both overt (public disinformation) and covert (hidden cyber and

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

infrastructure attacks, public opinion shaping), will almost certainly continue to evolve as an issue of national security in unprecedented ways (Hammond-Errey, 2016).

The digital landscape we rely on for economic growth, political stability and social interaction has created an ecosystem that is vulnerable to information influence and interference at individual and national levels (Hammond-Errey, 2022). People live a significant portion of their lives online and increasingly across the architectures of AI. This has the capacity to shape an individual, including what they see, what their options are, what choices they have, what they think others believe, and ultimately how they view the world (Hammond-Errey, 2024). Fragmented media landscapes and precise targeting lead to an increase in political and social polarisation (Prummer, 2020). An evolving technology landscape, AI, and algorithmic content curation, as well as increased foreign interference efforts, worsen the outlook.

Despite their ubiquity, understanding precisely how information and social media platforms impact public opinion remains difficult (Bradshaw & Howard, 2017), including in resort-to-force decision making. It is, however, clear that the strategies and techniques used by malign actors have an impact, and that their activities violate the norms of democratic practice (Bradshaw & Howard, 2018). "The computational architecture underpinning major social media platforms has so many parts as to defy understanding by any individual inquirer"(Lazar, 2024, nfd). Large technology companies create, use and control vast troves of personal data (Birch & Bronson, 2022). They have billions of users (Kemp, 2023) from whom they collect data and over whom they also have varying degrees of influence (Davidson, 2017; Griffin, 2019; Zuboff, 2019). They deploy complex systems involving layers of human content moderation, platform design and amplification algorithms that integrate standard programming, machine learning (ML) models, user interface design and vast amounts of data, from both on-platform behaviour and tracked behaviour online (Lazar, 2022).

There is an urgent research need to explore how influence and interference work at the cognitive level on contemporary information platforms and how big data and AI can influence behaviour (Hammond-Errey, 2024; Grahn, Häkkinen, & Taipalus, 2024). Cognitive processes and vulnerabilities such as perception and attention, emotion, decision making, memory metacognition, trust and cognitive bias can be exploited in the digital ecosystem (Grahn & Pamment, 2024). Since the broader concept of influence refers to the shaping of people's thoughts, beliefs and perceptions of the world, it is important to gain a greater understanding of how mental and psychological processes contribute to individuals' susceptibility to such influence (Grahn & Taipalus, 2025). This includes, for instance, understanding how people process, store and retrieve information; how cognitive biases affect decision making; and how emotion impacts judgment. By advancing such understanding, cognitive science can contribute to a deeper comprehension of how disinformation influences human behaviour (Grahn & Pamment, 2024).

Foreign influence and interference psychologically target individuals to influence or manipulate and alter perceptions of events by distorting the information environment in ways that benefit the sender of the information (Starbird, Arif & Wilson, 2019; Pamment & Isaksson, 2024). Such actions work by reshaping individuals' cognitions, or the mental frameworks people use to understand, interpret and respond to the world around them (Grahn & Pamment, 2024). The technology-fuelled digital landscape "allows … entities to utilise cyberspace to conduct operations that are tactically and strategically similar and also lowers the costs of collaboration between foreign and domestic malign entities" (Dowling, 2021). Conflicts are increasingly waged in digital environments and within the cognitive realm of individuals' minds (Bērziņš, 2019; Tashev, Purcell & McLaughlin, 2019).

The use of AI in social media is changing the political equation of public support and accumulating power in the technology companies that can, often opaquely, wield that power in their provision of social media platforms. The focus of AI in social media is narrowed in this context to include the

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

algorithms used for content discovery, curation, and moderation.[12] However, it is situated as part of the broader "information environment,"[13] which comprises informational, cognitive and physical dimensions (GAO [US Government of Accountability Office], 2022) in an attempt to understand "how human beings use information to influence the direction and outcome of competition and conflict" (Ehlers & Blannin, 2020). Using propaganda and information to influence the cognitive capacities of individuals is used by a range of hostile actors for warfare, radicalisation, and disinformation (Claverie, 2025). Cognitive processes such as attention, memory and emotional responses are often exploited by influence operations, and understanding these processes offers insight into points of vulnerability (Grahn & Pamment, 2024).

The information environment provides a useful framework for understanding information and technology challenges in three prongs: information or content – the information itself; digital landscape or infrastructure – the platforms and systems of creation, distribution and use; and cognitive or human resilience – our own engagement with information and the social context within which it's embedded (Hammond-Errey, 2022). The information environment "encompasses everything from human influence right through to information warfare, from peacetime to acute, large-scale conflict" (Hammond-Errey, 2022, np). Many aspects of the information environment impact deliberations on resort to force. The concept of the information environment is vital because it is a reminder that to influence public opinion, content alone is not enough. To be effective, attempts to influence public opinion must have some cognitive impact or influence. Taken in conjunction with the concentration of power in the architectures of AI and the capacity to impact real-world decisions and public opinion at once, this represents unprecedented change.

The capacity of social media and news media companies to influence our information environment is undeniable. In the context of content moderation, Donovan (2019) writes, "At every level of the tech stack, corporations are placed in positions to make value judgments regarding the legitimacy of content, including who should have access, and when and how." While most of the conversation about AI and mis- and disinformation revolves around content moderation, its impact is limited until it is distributed (Hammond-Errey, 2024c). Thus, sharing information is an essential consideration of AI and public opinion. This explains why the lens of the tech stack is so valuable. Looking at the infrastructure dimension of the information environment highlights how the internet infrastructure globally has become an "emerging terrain of disinformation" (Bradshaw & Denardis, 2022). The technical structure of social media platforms leaves users vulnerable to information influence and interference (Hammond-Errey, 2019), including from foreign actors and algorithmic processes. Social media can be used to erode trust in political institutions; to spread harmful disinformation; and to incite hate, polarisation, and anti-democratic sentiment (Khalil, 2024).

Most Australians are using social media and increasingly use it to access their news.[14] The market share of services used by adult users (age 16–64) is increasingly narrow in sectors such as search, where Google accounts for 94.5 percent of the share (Digital 2024, 2024, p.41), and in social media, where Meta dominates (Facebook, WhatsApp, and Instagram).[15] This means that their ability to shape

[12]Social media platforms use a variety of techniques, mostly focused on engagement to exert influence over their users. These include algorithmic discovery, which increases the influence and editorial power apps have over user experiences and content. Social media platform algorithms weight some features and characteristics differently among a wide array of features including interests, locations, likes and preferences, and social connections such as followers and friends.

[13]The term information environment, originally a military term, has been the subject of many independent works. An oft quoted US military doctrine defines the Information Environment is "the aggregate of the individuals, organizations, and systems that collect, process, disseminate or act on information." Joint Publication 3-13, Information Operations. US Defense Technical Informational Center, 27 November 2012, Incorporating Change July 2018.

[14]In Australia, with a population of 26.57 million people, there are 33.59 million mobile connections (126.4% of population), 25.31 million individuals using the internet (94.9% of population) and 20.80 million social media identities (78.3% of population) (Digital 2024, 2024, p. 19).

[15]The following percentage of Australians are users for the following platforms: Facebook (78.2%), Facebook Messenger (69.9%), Instagram (62.4), WhatsApp (44.8%), TikTok (40%), iMessage (39.6%), Snapchat (33%) and X (29.6%) (Digital 2024,

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

audiences' thinking and influence behaviour is high, as are their data collection capabilities. Social media saturation is very high, with almost all Australians using social media services.[16]

Social media platforms use a variety of techniques, mostly focused on increasing engagement, to exert influence over their users. These include algorithmic discovery and recommender systems, which increase the influence and editorial power applications and platforms have over user experiences, including the content they see. Some social media platforms, such as TikTok, weigh algorithms more heavily towards interests (and interest categories) rather than social connections, like followers and friends, as Facebook does (Hammond-Errey, 2024b). The weighting of algorithms is important as this significantly impacts user experience, including content selection and information "bubbles," however, they are largely opaque to the user and constantly evolving.

Given increased political polarisation as well as social media influence and interference – including in the context of the Israel-Hamas/Gaza conflict – the ability to obtain and maintain public support for military action includes a serious social media dimension. Given the opacity of social media algorithms, it is extremely difficult to conduct research. However, an example of public opinion regarding who shot down MH17 is indicative of the power of censored media over public opinion. In 2014 in Russia, where information is heavily mediated by the state, 97 percent of Russians did not believe Russian separatists were responsible for shooting down MH17, almost the inverse of public opinion globally (Luhn, 2014). Social media platforms are actively shaping public opinion about conflict and influencing what users can see, shaping their perceptions about whether governments can and should resort to force. In short, technology companies are moderating, shaping, influencing and ultimately gaining power and control over public opinion.

7. Discussion and implications for policymakers

The thesis of this article is that the role of AI in concentrating power, diffusing national security decision making, and shaping public opinion alters the political calculus and practical realities of going to war. There are key policy implications and considerations that follow from this, primarily focused on the imperative to improve understanding of the architectures of AI, the technology stack, and how they impact deliberations on the use of force.

Policymakers need an increased understanding of the tech stack as well as the inherent interdependencies and vulnerabilities in the technology ecosystem and the fragility of the architectures of AI. Based on this analysis, I recommend that technology literacy training programmes be designed specifically for politicians as well as policy, intelligence and military leaders. Moreover, this should be delivered by independent organisations. I also recommend that government and Defence invest in mapping the architectures of digital infrastructure and AI capabilities within their borders and regions. Moreover, governments should invest in research to develop a comprehensive picture of the physical and digital architectures of AI, including critical dependencies and vulnerabilities for Australia, our allies and the region, and inform how access and power are distributed. Governments should also fund the forecasting of future technology dependencies, specifically for their national government, defence forces and intelligence functions, in the next 2-5 years but also in longer term investments.

There is an urgent need to significantly increase awareness of government reliance on the architectures of AI, especially for critical government functions and functions of war. I recommend that

2024, p. 24). Facebook remains the favourite platform for nearly one in four Australians, who spend an average of 20 hours and 15 minutes per month. Twenty years after its launch, Facebook is still the leading social media platform in Australia (Digital 2024, 2024). Digital 2024 Australia also reports that TikTok has the highest average time per Android user of any social app, with 42 hours and 13 minutes per month – equating to almost one and a half hours per day using the platform. In second place is YouTube, with the average user spending 21 hours and 36 minutes per month on its Android app. Australians stand out among top economies as the users spending the most time on Snapchat, with 17 hours and 2 minutes and 619 sessions per month. That means that users open the Snapchat app over 20 times a day (Digital 2024, 2024).

[16]Ibid.

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

government, military and intelligence leadership be educated about these through research, establishment of advisory boards, forums and professional training. It is also recommended that intelligence agencies increase intelligence collection on critical and potential capabilities and that independent technical advisors are appointed, funded and security cleared to support intelligence agencies in this task. Without this, future government decision making will likely be constrained. Governments need to increase national investment to build public sovereign capabilities where needed. I also recommend governments invest in understanding now in further understanding biology and technology intersections to create safe and secure cyber physical systems over the horizon. Developing cognitive resilience in Australian leaders and people will be vital for national survival.

An increase in emerging technology literacy is urgently needed across governments. I recommend that governments immediately prioritise increasing their depth and scope of understanding of technology ecosystems, policies, and impacts on governing, security, warfare and public safety. This increase in awareness must include technology developments, the role of technology policy in Australia and globally, and the role that multi-lateral technology forums play in affecting AI capabilities and dependencies across the whole of government. This must be delivered by organisations that reflect technical and security expertise, are independent and include a technology ecosystem perspective as well as consideration of social harms and national security threats. This must occur immediately, or the window for shaping this ecosystem will be lost.

More research on social media and its impact on human cognition as well as the functions of government is urgently needed. Governments need to invest heavily in research, including research on democracy, the use of the information environment to influence public decisions on resort to force, and on foreign interference. I recommend that governments ensure data is available from social media platforms for this research, either through negotiation or regulation. Moreover, I recommend that funding for this research be made available to a wide range of researchers, civil society groups and academic institutions and consortiums to ensure it is representative of state demographics. There is an urgent research need to explore how foreign influence, and interference works at the cognitive level on contemporary information platforms and how AI can be used to understand and influence people's behaviour. I recommend governments invest immediately in research that reveals how cognitive processes and vulnerabilities (such as perception and attention, emotion, decision making, memory metacognition and trust) as well as cognitive biases can be exploited by malign actors in the digital ecosystem. Governments must also be willing to ensure that algorithmic processes as well as internal policies and procedures within social media service providers contribute to, or are at least consistent with the democratic principles of the country of sale. This is essential and requires immediate action.

8. Conclusion

This article has demonstrated how the architectures of AI – encompassing data, connectivity, energy, compute capacity and workforce – are consequential for the independent and sovereign decision making of governments on matters of war and peace. By concentrating power and diffusing national security decision making, and by shaping public opinion through AI-driven platforms, technology companies have emerged as national security actors. The scope and concentration of power within these firms mean that most nation states possess, or will soon possess, less autonomy in resort-to-force decisions, whether through direct coercion, indirect influence or strategic incentives.

The power asymmetries between governments and technology companies continue to grow, challenging a foundational principle of state sovereignty: the independent authority to declare and wage war. If nation states are to retain their sovereign independence in this domain, significant political will and urgent action are required. Policymakers must develop a deeper understanding of the interdependencies and vulnerabilities inherent in the technology ecosystem and devise strategies to contain the influence of private companies.

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

Competing interests. The author declares none.

Funding statement. The author declares none.

References

Ahmed, N., Muntasir Wahed, & Thompson Neil C (2023). The growing influence of industry in AI research. *Science 379*, 884–886. https://doi.org/10.1126/science.ade2420

Amazon. (2023). 2022 Amazon Annual Report. Amazon.com Inc., 25 January. Retrieved April 20, 2023, from https://ir.aboutamazon.com/annual-reports-proxies-and-shareholder-letters/default.aspx

Andrejevic, M. (2013). *Infoglut: How too much information is changing the way we think and know*. Routledge.

Bell, G. (2018). The character of future indo-pacific land forces. *Australian Army Journal*, *XIV*, 171–184.

Bergengruen, V. (2024) How Tech Giants Turned Ukraine Into an AI War Lab, Time. Retrieved September 20, 2024, from https://time.com/6691662/ai-ukraine-war-palantir/

Berzins, J. (2014). 'Russia's New Generation Warfare in Ukraine: Implications for Latvian Defense Policy', *Policy Paper 2* (National Defence Academy of Latvia Center for Security and Strategic Research).

Bērziņš, J. (2019). Not 'Hybrid' but New Generation Warfare. In *Russia's Military Strategy and Doctrine* (pp. 157–184). The Jamestown Foundation.

Birch, K., & Bronson, K. (2022). Big Tech. *Science as Culture*, *31*(1), 1–14. https://doi.org/10.1080/09505431.2022.2036118

Bode, I. (2023). Practice-based and public-deliberative normativity: Retaining human control over the use of force. *European Journal of International Relations*, *29*(4), 990–1016. https://doi.org/10.1177/13540661231163392

Bradshaw, S., & Denardis, L. (2022). Platform Governance: Internet Infrastructure as an Emerging Terrain of Disinformation, July 4, 2022, Centre for International Governance Innovation. https://www.cigionline.org/the-four-domains-of-global-platform-governance/

Bradshaw, S., & Howard, P. N. (2017). *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. The Computational Propaganda Project. Retrieved from http://comprop.oii.ox.ac.uk/research/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/

Bradshaw, S., & Howard, P. N. (2018). Why does Junk News Spread So Quickly Across Social Media? Algorithms, Advertising and Exposure in Public Life. Knight Foundation Working Paper. Retrieved from https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/142/original/Topos_KF_White-Paper_Howard_V1_ado.pdf

Bratton, B. H. (2015). *The stack: On software and sovereignty*. MIT Press.

Bresnick, S., Luong, N., & Curlee, K. (2024). Which Ties Will Bind? *Center for Security and Emerging Technology*. February 2024 https://doi.org/10.51593/20230037

Capaccio, A. (2023). Elon Musk's SpaceX Wins Pentagon Deal for Starlink in Ukraine. Bloomberg, 2 June. Retrieved June 13 2023, from https://www.bloomberg.com/news/articles/2023-06-01/musk-s-spacex-wins-pentagon-deal-for-its-starlink-in-ukraine#xj4y7vzkg

Claverie, B. (2025). Cognitive warfare: The new battlefield exploiting our brains, Polytechnique insights.

Cohen, J. E. (2017). Law for the platform economy. *University of California, Davis Law Review*, *51*, 133–204.

Collins, C., Dennehy, D., Conboy, K., & Mikalef, P. (2021). Artificial intelligence in information systems research: A systematic literature review and research agenda. *International Journal of Management*, *60*, 1–17.

Coveri, A., Cozza, C., & Guarascio, D. 2025. (2025). Big tech and the us digital-military-industrial complex. *Intereconomics*, *60*(2), 81–87. https://doi.org/10.2478/ie-2025-0017.

Crain, M. (2016). The limits of transparency: data brokers and commodification. *New Media & Society*, *20*(1), 88–104.

Daigle, B. (2021). 'Data Centers Around the World: A Quick Look', *United States International Trade Commission*, May, accessed 28 November 2023, https://www.usitc.gov/publications/332/executive_briefings/ebot_data_centers_around_the_world.pdf

Davidson, D. (2017). Facebook targets 'insecure' young people. The Australian, 1 May. Retrieved May 12, 2023, from https://www.theaustralian.com.au/business/media/facebook-targets-insecure-young-people-to-sell-ads/news-story/a89949ad016eee7d7a61c3c30c909fa6

Deeks, A., Lubell, N., & Murray, D. (2019). Machine learning, artificial intelligence, and the use of force by states. *Journal of National Security Law and Policy*, *4*, 1–25.

Department of Industry, Science and Resources. (2024). *Supporting responsible AI: discussion paper*, p. 5. Retrieved May 25, 2024, from, https://consult.industry.gov.au/supporting-responsible-ai

Digital 2024. (2024). We are Social, Australia (p. 19). Retrieved September 20, 2024, from https://wearesocial.com/au/blog/2024/01/digital-2024/

Donovan, J. (2019). Navigating the tech stack: When, where and how should we moderate content? *Centre for International Governance Innovation*. Retrieved September 20, 2024, from https://www.cigionline.org/articles/navigating-tech-stack-when-where-and-how-should-we-moderate-content/

Dowling, M. E. (2021). Foreign interference and Australian electoral security in the digital era. *Australian Journal of International Affairs*, *76*(1), 40–56.

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means. *Research Policy*, *52*(6). https://www.sciencedirect.com/science/article/pii/S0048733323000495?via%3Dihub

Edward, W. (2020). The Uberisation of work: The challenge of regulating platform capitalism. A commentary. *International Review of Applied Economics*, *34*(4), 512–521.

Ehlers, R., & Blannin, P. (2020). Making Sense of the Information Environment. *Small Wars Journal*. Retrieved September 10, 2023, from https://smallwarsjournal.com/jrnl/art/making-sense-information-environment

Eichensehr, K. (2019). Digital Switzerland. *University of Pennsylvania Law Review*, *167*, 665.

Erskine, T. (2024). *Before* algorithmic Armageddon: Anticipating immediate risks to restraint when AI infiltrates decisions to wage war. *Australian Journal of International Affairs*, *78*(2), 175–190. https://doi.org/10.1080/10357718.2024.2345636

Erskine, T., & Miller, S. E. (2024). AI and the decision to go to war: Future risks and opportunities. *Australian Journal of International Affairs*, *78*(2), 135–147. https://doi.org/10.1080/10357718.2024.2349598

Fernandez, R., Klinge, T. J., Hendrikse, R., & Adriaans, I. (2021). How big tech is becoming the government. Tribune, 5 February. Retrieved March 22, 2022, from, https://tribunemag.co.uk/2021/02/how-big-tech-became-the-government

Galeotti, M. (2016). Hybrid, ambiguous, and non-linear? How new is Russia's 'new way of war'?. *Small Wars & Insurgencies*, *27*(2), 282–301.

Ganz, A., Camellini, M., & Hine, E. (2024). Submarine cables and the risks to digital sovereignty. *Minds and Machines*, *34*, 31. https://doi.org/10.1007/s11023-024-09683-z

GAO [US Government of Accountability Office]. (2022). Information Environment, Opportunities and Threats to DOD's national Security Mission (GAO-22-104714). Retrieved September 2023, from https://www.gao.gov/assets/gao-22-104714.pdf

Gawer, A. (2022). Digital platforms and ecosystems: remarks on the dominant organizational forms of the digital age. *Innovation*, *24*(1), 110–124.

Giles, K. (2023). Tech giants hold huge sway in matters of war, life and death. That should concern us all. The Guardian. 12 Sep 2023 https://www.theguardian.com/commentisfree/2023/sep/12/tech-giants-war-elon-musk-ukraine-starlink

Grahn, H., Häkkinen, T., & Taipalus, T. (2024). Cognitive Security in a Changing World: Citizen Perceptions During Finland's NATO Joining Process. In M. Lehto (Ed.), *Proceedings of the 23rd European Conference on Cyber Warfare and Security* (23, 165–171).

Grahn, H., & Pamment, J. (2024). *Exploitation of psychological processes in information influence operations: Insights from cognitive science*. Lund University, Psychological Defence Research Institute Working Paper, 2024:4.

Grahn, H., & Taipalus, T. (2025). Defining Comprehensive Cognitive Security in the Digital Era: Literature Review and Concept Analysis. *Journal of Information Warfare*, *24*(2), 39–59. https://www.jinfowar.com/journal/volume-24-issue-2/defining-comprehensive-cognitivesecurity-digital-era-literature-review-concept-analysis

Greene, A. (2024). Amazon wins contract to store 'top-secret' Australian military intelligence. ABC. 4 Jul 2024 https://www.abc.net.au/news/2024-07-04/amazon-contract-top-secret-australian-military-intelligence/104057196

Griffin, P. (2019). Facebook won't give up its insidious practices without a fight. Noted, 22 March.

Gyngell, A., & Wesley, M. (2007). *Making Australian foreign policy* (2nd ed.). Cambridge: Cambridge University Press.

Hammond-Errey, M. (2016) *Information Influence* in an Era of Global Insecurity and Digital Connectivity (Russian Disinformation Strategies and Hybrid War: Implications for Government and National Security Operations) Master's Thesis, ANU

Hammond-Errey, M. (2017) 28 September 2017, A Perpetual Conflict of Ideas? *Strategy Bridge* https://thestrategybridge.org/the-bridge/2017/9/28/a-perpetual-conflict-of-ideas

Hammond-Errey, M. (2019). Understanding and Assessing Information Influence and Foreign Interference. *Journal of Information Warfare*, *18*(1), 1–22. Winter 2019.

Hammond-Errey, M. (2022). *Dealing with disinformation: A critical new mission area for AUSMIN*. United States Studies Centre. 5 December 2022.

Hammond-Errey M. (2023). *Building the Quad Technology Workforce Pipeline and Research Relationships*. ANU National Security College. Retrieved November 20, 2023, from https://nsc.crawford.anu.edu.au/publication/21660/building-quad-technology-workforce-pipeline-and-research-relationships

Hammond-Errey, M. (2024). *Big Data, Emerging Technologies and Intelligence: National Security Disrupted*. United Kingdom: Routledge.

Hammond-Errey, M. (2024b). Should Australia ban TikTok?, 18 June 2024, Lowy Interpreter, https://www.lowyinstitute.org/the-interpreter/byte-sized-diplomacy-should-australia-ban-tiktok

Hammond-Errey, M. (2024c). Understanding technology as an ecosystem is the first step to tackling online harms, 22 Oct 2024, Lowy Interpreter, https://www.lowyinstitute.org/the-interpreter/understanding-technology-ecosystem-first-step-tackling-online-harms

Hammond-Errey, M. (2025). Meta power move is about more than fact checking. Lowy Interpreter 15 Jan 2025, https://www.lowyinstitute.org/the-interpreter/meta-power-move-about-more-fact-checking (accessed 15 Jan 2025).

Harwell, D. (2025). Trump vilified tech giants. Now they're giving him millions. Washington Post. January 11, 2025. https://www.washingtonpost.com/technology/2025/01/11/trump-big-tech-inauguration-zuckerberg-bezos-google/ (Last accessed 18 Jan 2025)

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

Hendell, G. (2023). The Use of Force by States Under International Law. Available at: https://theforge.defence.gov.au/article/use-force-states-under-international-law (Accessed: 11 July 2024).

Herbert, L., & Kerr, J. (2021). On Cyber-Enabled Information Warfare and Information Operations. https://doi.org/10.1093/oxfordhb/9780198800682.013.15.

Hershkovitz, S. (2022). *The Future of National Intelligence*. Lanham, MD: Rowman and Littlefield. 2022

Hoffman, F. G. (2007). *Conflict in the 21st century: The rise of hybrid wars*. Arlington, Virginia: Potomac Institute for Policy Studies).

Hoffman, F. G. (2016). The Contemporary Spectrum of Conflict: Protracted, Gray Zone, Ambiguous, and Hybrid Modes of War. In *2016 Index of U.S. Military Strength*. (p. 26). The Heritage Foundation.

Horowitz, J. (2023). Digital Tech Companies in War: What is the Law? What are the Risks? October 13 2023. https://www.justsecurity.org/89463/digital-tech-companies-in-war-what-is-the-law-what-are-the-risks/

Horowitz, J. (2024). One click from conflict: Some legal considerations related to technology companies providing digital services in situations of armed conflict. *Chicago Journal of International Law*, *24*(2), 305–337.

Howell, B. E., & Potgieter, P. H. (2020). Politics, policy and fixed-line telecommunications provision: Insights from Australia. *Telecommunications Policy*, *44*(7), 1–19.

IEA [International Energy Agency]. 2025. Energy and AI, World Energy Outlook. Special Report. Retrieved September 02, 2025, from https://www.iea.org/reports/energy-and-ai

Kak, A., West, S. M., & Whittaker, M. (2023). Make no mistake—AI is owned by Big Tech, MIT Technology Review, December 5, 2023, https://www.technologyreview.com/2023/12/05/1084393/make-no-mistake-ai-is-owned-by-big-tech/

Kelly, L. (2025) Musk extends political tentacles into UK, Germany. The Hill. 6 Jan 2025 https://thehill.com/policy/international/5066254-musk-extends-political-tentacles-into-uk-germany/ (Accessed 7 Jan 2025).

Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E., & Troath, S. (2022). Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *International Affairs*, *98*(6), 1977–1999. https://doi.org/10.1093/ia/iiac226

Kemp, S. (2023). Digital 2023. We are social, 26 January. Retrieved April 05 2023, from https://wearesocial.com/au/blog/2023/01/the-changing-world-of-digital-in-2023-2/

Kent, S. (1966). *Strategic Intelligence for American World Policy*. 1966, p. vii. Princeton University Press

Khalil, L. (2024). Overcoming digital threats to democracy: Using deliberative democracy to enhance trust and legitimacy in digital spaces. *Lowy Institute*. 20 February 2024.

Khanal S., Zhang, H., & Taeihagh, A. (2024). Why and how is the power of Big Tech increasing in the policy process? *The case of generative AI Policy and Society*, *44*(1), 52–69. https://doi.org/10.1093/polsoc/puae012

Kind, C. (2024). On Technology & Security Podcast, hosted by Dr Miah Hammond-Errey. TS Episode 21, Privacy, data, AI and tech power with Australian Privacy Commissioner Carly Kind. Retrieved September 10, 2024, from https://miahhe.com/episode-21

Kitchin, R. (2014). *The data revolution: big data, open data, data infrastructures & their consequences*. London: SAGE.

Koslosky, L. (2023). Quad collaboration for STEM workforce growth. ANU National Security College. Retrieved November 20, 2023, from https://nsc.anu.edu.au/national-security-college/content-centre/research/quad-collaboration-stem-workforce-growth

Krasner, S. D. (1999). *Sovereignty: Organized Hypocrisy*. Princeton University Press, ProQuest Ebook Central.

Lazar, S. (2022). Legitimacy, Authority, and Democratic Duties of Explanation, Forthcoming in Oxford Studies in Political Philosophy. This version was presented to the Oxford Studies in Political Philosophy workshop, Tucson Arizona. October 2022.

Lazar, S. (2024). Legitimacy, Authority, and Democratic Duties of Explanation. In D. Sobel & S. Wall (Eds.), *Oxford Studies in Political Philosophy Volume 10, Oxford Studies in Political Philosophy (Oxford*. 2024 online edn Oxford Academic. 30 Apr. 2024).

Lee, J. (2021). Big data for liberal democracy. *The Australian, 5 March*. Retrieved March 12, 2022, from https://www.theaustralian.com.au/inquirer/big-data-for-liberal-democracy/news-story/10ed6d4d8b01677955fc468d3751a4b7

Lehdonvirta, V. (2022). *Cloud Empires: How Digital Platforms Are Overtaking the State and How We Can Regain Control*. Cambridge: MIT Press.

Lehdonvirta, V. (2023). 'The political geography of AI infrastructure,' *Oxford Internet Institute*, accessed 28 November 2023, https://www.oii.ox.ac.uk/research/projects/the-political-geography-of-ai-infrastructure/

Lehdonvirta, V., Wu, B., & Hawkins, Z. (2024). Compute North vs. Compute South: The Uneven Possibilities of Compute-based AI Governance Around the Globe. *Nature*. https://doi.org/10.31235/osf.io/8yp7z

Lerman, R. & Zakrzewski, C. (2022). *Elon Musk's Starlink Is Keeping Ukrainians Online When Traditional Internet Fails*. WASH. POST.

Libicki, M. (1995). *What is Information warfare?* National Defense University. Retrieved September 10, 2024, from https://apps.dtic.mil/sti/citations/tr/ADA367662

Lin, H., & Jaclyn, K. (2021). On Cyber-Enabled Information Warfare and Information Operations. In P. Cornish(Ed.), *The Oxford Handbook of Cyber Security, Oxford Handbooks* (2021 edn, pp. 251–272). Oxford Academic. Retrieved December 8 , 2021, from https://doi.org/10.1093/oxfordhb/9780198800682.013.15

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

Lotz, A. (2018, March 24). "Big tech" isn't one big monopoly – It's 5 companies all in different businesses. *The Conversation*. https://theconversation.com/big-tech-isnt-one-big-monopoly-its-5-companies-all-in-different-businesses-92791

Luhn, A. (2014). MH17: Vast majority of Russians believe Ukraine downed plane, poll finds, The Guardian UK. Retrieved December 2, 2015, from https://www.theguardian.com/world/2014/jul/30/mh17-vast-majority-russians-believe-ukraine-downed-plane-poll

Lushenko, P., & Carter, K. (2024) A new military-industrial complex: How tech bros are hyping AI's role in war, October 7, 2024, https://thebulletin.org/2024/10/a-new-military-industrial-complex-how-tech-bros-are-hyping-ais-role-in-war/

Metz, C. (2022). Elon Musk backtracks, saying his company will continue to fund internet service in Ukraine. The New York Times. Retrieved April 19 2023, from, https://www.nytimes.com/live/2022/10/15/world/russia-ukraine-war-news#musk-ukraine-internet-starlink

Moore, M. (2016). *Tech giants and civic power*. London: King's College London Policy Institute.

Moore, M., & Tambini, D. (Eds.). (2021). *Regulating Big Tech: Policy Responses to Digital Dominance*. Oxford University Press.

Neef, D. (2014). *Digital exhaust: What everyone should know about big data, digitization and digitally driven innovation*. Upper Saddle River, NJ: Dale Neef.

Neilsen, R., & Pontbriand, K. (2025). "Hands off the keyboard": NATO's cyber-defense of civilian critical infrastructure. *Defence Studies*, 519–542.

Nieberg, P. (2025). Army bringing in big tech executives as lieutenant colonels. Task and Purpose. https://taskandpurpose.com/military-life/army-reserve-lt-col-tech-execs

Nissen, T. E. (2015). *#TheWeaponizationOfSocialMedia- @Characteristics_of_ Contemporary_Conflicts*. Copenhagen, Denmark: Royal Danish Defence College).

Omand, D., & Phythian, M. (2018). *Principled spying: the ethics of secret intelligence*. Oxford University Press, Oxford.

Pamment, J., & Isaksson, E. (2024). Lund University Psychological Defence Research Institute Psychological Defence: Concepts and principles for the 2020s MPF REPORT SERIES 6/2024. https://mpf.se/psychological-defence-agency/publications/archive/2024-10-28-psychological-defence-concepts-and-principles-for-the-2020s

Perrigo, B. (2024). Exclusive: New Research Finds Stark Global Divide in Ownership of Powerful AI Chips, Time Magazine AUGUST 28, 2024 8:00 AM EDT. Retrieved September 10, 2024, from https://time.com/7015330/ai-chips-us-china-ownership-research

Prummer, A. (2020). Micro-targeting and polarization. *Journal of Public Economics*, *188*.

Quell, M. (2025). *Trump's sanctions on ICC prosecutor have halted tribunal's work*. AP News. Retrieved June 1, 2025, from https://abcnews.go.com/International/wireStory/trumps-sanctions-icc-prosecutor-halted-tribunals-work-121824057

Richmond, B. (2019). *A day in the life of data*. Melbourne: Consumer Policy Research Centre.

Rogers, Z., & Bienvenue, E. M. (2021). Combined Information Overlay for Situational Awareness in the Digital-Anthropological Terrain. *Cyber Defense Review*, 89–107. Summer 2021-2022.

Sadowski, J. (2020). *Too Smart: How Digital Capitalism is Extracting Data, Controlling Our Lives, and Taking Over the World*. MIT Press.

Santesteban, C., & Longpre, S. (2020). How big data confers market power to big tech: leveraging the perspective of data science. *Antitrust Bulletin*, *65*(3), 459–485.

Schaake, M. (2024a). *The Tech Coup: How to Save Democracy from Silicon Valley*. Princeton University Press.

Schaake, M. (2024b). Tech Companies aren't just going to war. They're owning the battlefield. Fast Company. Retrieved August 10, 2024, from https://www.fastcompany.com/91192057/tech-companies-arent-just-going-to-war-theyre-owning-the-battlefield

Schwarz, E. (2024). Unicorns for Uniforms: On the Problematic Allure of VC Investments in Defence, Opinio Juris. Retrieved August 10, 2024, from https://opiniojuris.org/2024/s09/18/unicorns-for-uniforms-on-the-problematic-allure-of-vc-investments-in-defence/

Seib, P. (2021). *Information at War. Journalism, disinformation and modern warfare*. Cambridge UK: Polity.

Selhorst, T. (2016). Russia's Perception Warfare: The development of Gerasimov's doctrine in Estonia and Georgia and its application in Ukraine. *Militaire Spectator*, 148–164. Jaargang 185 (Nummer 4 – 2016).

Shafiabady, N., & O'Neil, A. (2025). America first, ethics second: The implications of Trump's AI Executive Order, Lowy Institute. https://www.lowyinstitute.org/the-interpreter/america-first-ethics-second-implications-trump-s-ai-executive-order

Shalaby, M., & Tidy, J. (2024). Palestinians say Microsoft unfairly closing their accounts, BBC, 11 July 2024 https://www.bbc.com/news/articles/cger582weplo

Sommer, U., Matania, E., & Hassid, N. (2023). The rise of companies in the cyber era and the pursuant shift in national security. *Political Science*, *75*(2), 140–164. https://doi.org/10.1080/00323187.2023.2278499

Starbird, K., Arif, A., & Wilson, T. (2019). Disinformation as collaborative work: Surfacing the participatory nature of strategic information operations. *Proceedings of the ACM on human-computer interaction*, *3*(CSCW), 1–26.

Stone, P. (2024) Musk's conflicts of interest as Trump adviser could benefit him, experts warn. The Guardian. https://www.theguardian.com/technology/2024/dec/23/elon-musk-conflict-of-interest-benefits (Accessed 20 Jan 2025).

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press

Stucke, M., & Grunes, A. (2016). *Big Data and Competition Policy*. Retrieved November 03, 2025, from https://doi.org/10.1093/law:ocl/9780198788133.001.0001

Tashev, B., Purcell, M., & McLaughlin, B. (2019). 'Russia's information warfare: Exploring the cognitive dimension. *MCU Journal*, *10*(2), 129–147.

Thornton, R. (2015). The Changing Nature of Modern Warfare. *The RUSI Journal*, *160*(4), 40–48.

Tomz, M., Weeks, J. L. P., & Yarhi-Milo, K. (2020). Public opinion and decisions about military force in democracies. *International Organization*, *74*(1), 119–143. Retrieved August 10, 2024, from https://www.jstor.org/stable/26892862

Top500 2024. (2024). 'Lists, Top 500 June 2024, *Top500*, accessed 12 July 2024, 2023, https://www.top500.org/lists/top500/2024/06/

Tsaih, R. H., Chang, H. L., Hsu, C.-C., & Yen, D. (2023). The AI Tech-Stack Model. *Communication of the ACM*, *66*(3), 69–77. https://doi.org/10.1145/3568026.

UK Department for Science, Innovation and Technology. (2023). *Independent review of the future of compute: Final report and recommendations* (Led by Zoubin Ghahramani FRS). https://www.gov.uk/government/publications/future-of-compute-review/the-future-of-compute-report-of-the-review-of-independent-panel-of-experts#introduction-from-the-expert-panel

van Dijck, J., Poell, T., & de Waal, M. (2018). *The platform society: Public values in a connective world*. New York: Oxford University Press.

Verdegem, P. (2022). Dismantling AI Capitalism: The Commons as an Alternative to the Power Concentration of Big Tech. *AI & Society*, *39*, 727–737. https://doi.org/10.1007/s00146-022-01437-8

Watts, T. (2020). *Democracy and the authoritarian challenge*. Canberra: Lowy Institute. Retrieved August 10, 2024, from https://myaccount.lowyinstitute.org/events/2020-npc-tim-watts

Waxman, M. C. (2013). Regulating Resort to Force: Form and Substance of the UN Charter Regime. *European Journal of International Law*, *24*(1), 151–189.

Whelan, C., Hammond-Errey, M., & Villeneuve-Dubuc, M. (2024). ARTIFICIAL INTELLIGENCE: Analysis of AI Governance Frameworks for Law Enforcement, Australian cyber security cooperative research centre. July 2024.

White House. (2025). Winning the Race. AMERICA'S AI ACTION PLAN. Retrieved May 15, 2025, from https://www.whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf

Whitlark, R. E. (2021). *All Options on the Table: Leaders, Preventive War, and Nuclear Proliferation*. Cornell University Press).

World Bank. (2023). *GDP (current US$)*. The World Bank. Retrieved April 12, 2023, from https://data.worldbank.org/indicator/NY.GDP.MKTP.CD

Zegart, A. (2022). *Spies, Lies, and Algorithms: The History and Future of American Intelligence*. Princeton: Princeton University Press.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. London: Profile Books.

Dr Miah Hammond-Errey is the founding CEO of Strat Futures Pty Limited, host of the Technology & Security Podcast and an adjunct Associate Professor at Deakin University. She leads the development of a platform to improve cognitive readiness and resilience in leaders who make high stakes decisions. Dr Miah Hammond-Errey spent 18 years leading federal government analysis, operational and liaison activities in Australia, Europe and Asia. She has been awarded medals, citations and awards for operational service, leadership and excellence. Her book, *Big Data, Emerging Technologies and Intelligence: National Security Disrupted* (2024) is based on her PhD. She developed the *Information Influence and Interference (I3) Framework*, at ANU, to counter Russian disinformation. Previously, she established and led think tank programmes on emerging technologies and information operations. Dr Miah Hammond-Errey publishes and presents at the intersection of technology and security and teaches postgraduate students cyber security, emerging technologies and national security.

Cite this article: Hammond-Errey, M. (2025). Architectures of AI: Tech power broking war? *Cambridge Forum on AI: Law and Governance*, *1*, e44, 1–21. https://doi.org/10.1017/cfl.2025.10028

https://doi.org/10.1017/cfl.2025.10028 Published online by Cambridge University Press