SECURITY & DEFENCE QUARTERLY

https://securityanddefence.pl/

The new power model and United States national defence agility

Stephen R. Willis[1], **Kurt W. Jefferson**[2]

[1]swillis01@spalding.edu

[1]https://orcid.org/0009-0004-2729-5897

[1]Doctoral Program in Leadership, College of Education, Spalding University, Louisville, KY, USA

[2]kjefferson@spalding.edu

[2]https://orcid.org/0009-0009-6143-501X

[2]Dean of Graduate Education and Professor, Spalding University, 901 South 4th Street, 40203, Louisville, KY, USA

Abstract

This scholarly article provides a comprehensive analysis of how Heimans and Timms's (Heimans, J. and Timms, H. (2018) New power: How power works in our hyperconnected world—and how to make it work for you. New York, NY: Doubleday) principles of "new power" can be applied to enhance the agility and effectiveness of United States national defence strategies and policies. The analysis underscores the critical importance of fostering collective intelligence, adaptability, flexibility, transparency, and inclusion within the operations and decision-making processes of the US military, emphasising transparency and inclusion is crucial in promoting open source and open information exchange that involves service members and defence leaders at all levels in decision-making. This study presents compelling examples of how embracing new power dynamics can improve the agility of US national security efforts in terms of strategies and policies. Improved agility will potentially save lives and provide a competitive advantage over our adversaries. Additionally, the article highlights the significance of adaptability and flexibility in navigating the rapidly changing global landscape, underscoring the need for the US military to adapt to shifting power dynamics and embrace agility as a critical element in achieving success in the face of modern security challenges. Finally, this research delves into two critical areas: First, we explore a new power model for enhancing the agility of US national defence. Second, we discuss how the new power model can facilitate agile decision-making for US intelligence, specifically through the practice of open-source Intelligence. We conclude that making American national defence agile in its policies and strategies requires not only the application of new power principles and concepts, as Heimans and Timms (2018) understand them, but also the ability to apply new power in nuanced, incremental, and thoughtful ways that will allow for transformation of the defence and policy-making apparatus in a way that will be accepted and understood by policymakers and service members and leaders themselves.

Article info
Received: 9 November 2024
Revised: 4 March 2025
Accepted: 5 March 2025
Available online: 22 April 2025

Citation: Willis S.R. and Jefferson K.W. (2025) 'The new power model and United States national defence agility', *Security and Defence Quarterly*, 50(2).
doi: 10.35467/sdq/202643.

Keywords:

US national defence, new power, artificial intelligence (AI), military agility, open-source intelligence, leadership

Introduction

In an era where artificial intelligence (AI) is rapidly transforming every sector of society, national defence strategies must evolve to keep pace. Traditional defence models, which have been successful in stable, predictable environments, can no longer address the challenges posed by today's dynamic and constantly shifting global landscape. AI's exponential growth has created an environment where stability is the exception rather than the norm, and this paradigm shift applies not only to the United States but also to its adversaries, who are increasingly leveraging AI to enhance their military capabilities. As noted in the Department of Defense (2023, p. 3) data, analytics, and artificial intelligence adoption strategy, the rapid adoption of data and AI technologies presents a unique opportunity to "equip leaders at all levels of the [US] Department with the data they need and harness the full potential of decision-making." Consequently, the need for adaptable agile models in the US national defence has never been more critical.

The "new power" model, as articulated by Heimans and Timms (2018, pp. 14–18), offers a fresh approach that emphasises adaptability, transparency, and collective intelligence attributes, which are essential for navigating this era of rapid technological advancement. In traditional military strategies, decision-making processes were often slow and hierarchical, designed for a world where threats evolved gradually. However, AI is reshaping the rules of engagement, accelerating the pace of conflict and innovation. Consequently, traditional models have become insufficient in an environment that shifts continuously, often in unpredictable ways. The US military must embrace models that allow for quick decision-making, fluid adaptation to new threats, and the leveraging of collective intelligence across all levels of its operations. As AI continues to drive change, frameworks like the new power model for US National Defence Agility will become mission-critical. These models empower decision-makers with real-time, open-source intelligence (OSINT), foster inclusivity in military decision-making, and create avenues for rapid adaptation in the face of emerging threats. To underscore the importance of this shift, consider this: "We are now with AI, where the Internet was in 1995." Just as the Internet revolutionised communication, commerce, and defence strategies in the late 20th century, AI is poised to do the same in our current era but at an even faster pace. In 1995, the Internet was largely unregulated, unstructured, and full of untapped potential. Those who quickly adapted to its possibilities reaped extraordinary benefits. Today, we stand on the precipice of a similar transformation with AI, and the US military must be ready to adapt swiftly. If we fail to evolve our strategies in tandem with AI's rapid development, we risk losing the technological and strategic edge to our adversaries.

It is crucial to delve into the existing body of research on AI's role in modern warfare to set the stage for a more comprehensive understanding of how AI-driven models, in the context of the new power model, can enhance national defence. The following literature review will explore how AI integration, alongside agile frameworks, may be reshaping defence strategies and positioning the United States to address evolving threats more effectively.

Literature review

The necessity of Heimans and Timms's (2018) new power model in the US national defence arises from the unprecedented pace of advancement in AI. Gibson and Jefferson (2022) discussed Heimans and Timms's model and opined that "new power" is a set of values that are qualitatively different from "old power" values. Old power is hierarchical, top-down, based on political, social, and economic structures of the past that value control and order. Old power is "formal-representative-governance, managerialism, institutionalism," "competition, exclusivity, resource consolidation," "confidentiality, discretion, separation between private and public spheres," "expertise, professionalism, specialisation," and "long-term affiliation and loyalty and less overall participation." New power values include "informal networks," "opt-in decision-making," "self-organisation," "collaboration, crowd wisdom, sharing, open-sourcing," "radical transparency," "maker culture," a "do-it-ourselves" ethic, increased participation, and "short-term conditional affiliation" (Gibson and Jefferson, 2022, p. 30). Jefferson *et al.* (2021) used an example to show how agility and the new power model were applied in government to change the *status quo* and demonstrate the ossification of old power structures and the advent of a new decision-making approach that lent itself to new power application and outcomes.

Heimans and Timms (2018, pp. 14–18) used the National Aeronautics and Space Administration (NASA) as an example of old power and how its scientists began to recognise the decay of its old power-like processes. At NASA, courageous professionals took advantage of modern communication platforms by soliciting advice from the public. NASA officials then disseminated more than a dozen research and development challenges for public analysis. Thereafter, they received thousands of credible responses from private persons in eighty countries from around the world. It was stated that, on average, it would take the Research and Development (R&D) team at NASA 3–5 years to resolve the problems. However, by using an open platform, the problems were resolved faster with the help of those outside the NASA community. This new collaborative approach took 3–6 months. This is just one of the many examples of shifts in power, which took root nearly a decade ago (Jefferson *et al.*, 2021, p. 3).

The application of new power is important for understanding how decision-making in defence policy-making is evolving. Heimans and Timms (2018, pp. 28–32 & pp. 48–50) argue that the effect of the new power model has been felt in the expansion of participation in both Western and non-Western contexts. In this regard, Gibson and Jefferson (2022, p. 30) state as follows:

> Heimans and Timms recognise the importance of "new power" and warn that new power for socially just ends in crowdsourcing via social media can also be used by enemies of the United States and the West: New means of participation—and the heightened sense of agency that has come with them—are a key ingredient in some of the most impactful models of our time: big businesses like Airbnb and Uber, China's WeChat or Facebook; protest movements like Black Lives Matter; open software systems like GitHub; and terrorist networks like ISIS. They are all channeling new power.

Numerous scholars and defence experts have examined AI's implications for modern warfare and strategy. The necessity for the new power model in US national defence arises from the unprecedented advancements in AI. Numerous scholars and defence experts have examined the implications of AI on modern warfare and strategy. Mikhailov (2023, p. 1) emphasises the transformative role of AI in military operations, stating that "artificial intelligence presents unparalleled opportunities for strengthening our defence capabilities." His analysis underscores the need for military leaders to recognise AI's strategic importance and integrate these technologies into decision-making processes, emphasising that AI will serve as a force multiplier in augmenting existing capabilities and enabling novel operational concepts. This insight directly supports the new power model's emphasis on leveraging advanced technologies, adaptability, and decentralised decision-making to enhance national defence agility. Mikhailov's work also highlights the integration of AI into military operations through frameworks that account for the model, data, and computing environment. He states that "deploying AI systems in battlespace contexts requires careful consideration of three main components: the model, data, and computing environment," which aligns with the new power model's focus on real-time decision-making and collective intelligence. The ability to quickly process vast amounts of data from diverse sources, such as satellite imagery and field reports, directly parallels the principles of OSINT, a key element of the new power model. Moreover, Mikhailov's perspective that AI will "revolutionise military operations, serving as a force multiplier that augments existing capabilities and enables the development of novel operational concepts" supports the idea that AI-driven decision-making will significantly improve the agility of US national defence strategies. Implementing advanced AI-driven frameworks can foster rapid adaptation to evolving threats, a core tenet of the new power model for the US national defence agility.

Although the deployment of AI-based decision-making and technology may improve agility, the use of AI-based weaponry in conflict may raise ethical and other alarm bells in the battlespace in direct combat. Burnett and Jefferson (2024, p. 200) quote Mike Walsh, the author of *The Algorithmic Leader* (2019):

> Hackers, terrorists, and rogue states will influence the agenda by raising the digital threat level. Regulators, politicians, and other government authorities will seek to define and protect their own position as public awareness grows. Given these challenges, Google's former unofficial motto, "Don't be evil," seems both prescient and naïve.

According to Moreno *et al.* (2022), even the assumptions on which research in warfighting and AI-enabled technologies are based are complicated, and the potential ramifications are broad, deep, and fluid (and, in some aspects, unknown). As Moreno *et al.* (2022) argue, even the neuroscience around the research provides "novel challenges" to the research on conflict and ethics. They state that the neuroscience behind AI-driven warfighting technology must not only conform to ethics in research protocols on human subjects but also begin to integrateethics in assumptions tied to research and participants in military clinical research, such as basic neuroscience and its applications,whichcould violate ethical standards of human subject research.

"Neuroenhancement" marries such life sciences as neurology, pharmacology, genetics, and psychology with long-time soldiering attributes that include endurance, speed, intelligence-gathering, targeting, and training, none of which are medical conditions. As with any military technology, neuroenhancement products move slowly from research and development to field use (Moreno *et al.*, 2022).

Clinical researchers will have to show *prima facie* evidence of the "value of their research" and dovetail that value with justifications that show an overriding concern for ethics in terms of both humans and warfighting (Moreno *et al.,* 2022). With regard to actual combat, the ethics of AI in the battlespace has been playing out in front of the world in both the 2022 Russo-Ukraine War and the fifth Israel-Hamas War (which started in 2023). The former was the first "large-scale" war involving the use of unmanned aerial vehicles (UAVs) on both sides. "Drones were being used to by both sides to monitor troop movements, attack air forces, target citizens, and attack military and civilian installations" (Burnett and Jefferson, 2024, p. 203). Regarding "the 2023 Israel-Gaza war, by November 2023, some 11,000 targets had been struck by the IDF [Israel Defense Forces] in northern Gaza alone" (Burnett and Jefferson, 2024, p. 204). Baker (2024) has argued that ethics, as a crucial framework for decision-making and application of AI, will continue to evolve in the field of national security law. He states that law has a difficult time keeping up with technology. Also, Baker (2024) believes that applying ethical standards to the general context of generative AI and technological transformation will be a better way to deal with the ethical problems of AI than regulating "specific types or attributes of technology." Baker (2024, p. 95) argues that "ethics, if applied, might fill the vacuum left by incomplete or inadequate legislation or the absence of legislation."

Rowe (2022) argues that not all ethical issues surrounding AI on the battlefield are due to the technology itself. He offers suggestions to understand *en toto* the problem of blaming AI for ethical violations of warfighting. Some of the issues are human-created, but ethical issues can result from the machines themselves, regarding computing problems, network issues, and data management. However, he goes on to say that "mitigation" is the key. In his opinion, "it is important to assess how each AI method works to see how well its contribution to lethal force can be justified, and the methods differ considerably in their accuracy and explainability, and hence their possible justifiability." Further, he believes that having the ability to employ ethical checks and pathways in the systems themselves, as well as "testing software" to understand where the ethical lapses may be, will assist in making the ethics questions more answerable and the entire decision-making process more transparent. The negatives of AI have emerged in the workplace and in the battlespace. In this regard, the rector of the United Nations University, Dr. Tshilidzi Marwala (2023), states as follows:

> How, for example, can we guarantee that AI systems are impartial and do not perpetuate existing biases? How can we ensure that AI decision-making mechanisms are transparent? How can we safeguard privacy when AI systems frequently rely on vast data? How do we get people who understand the technical and regulatory frameworks? How do we bridge the gap between the AI haves and the AI have-nots?

Marwala (2023) points out the issues with overall governance of machine-learning and with AI evolution in general. The use, regulation, and future applications of AI hang in the balance, and without a general framework of governance at the transnational level, Marwala fears that the use of AI in conflicts "raise concerns regarding the escalation of conflicts, the possibility of autonomous weapons being compromised or misused and the possibility of an AI arms race." Although AI has many positive potential uses, ranging from "quicker decision-making" to "more accurate targeting," the downsides could outweigh the upsides.

Block (2023) discusses the history of OSINT gathering in his study of the long-evolving practice. From the 19th century, forms of OSINT have been used by various governments (as we discuss below regarding its use by the Israelis in intelligence, military affairs, and battle-fighting). Block states that "with the coming of the information age in particular, the rise of the Internet and the digital domain for production and storage of information, the nature and volume of publicly available information has changed fundamentally." Block studied the use of OSINT in the American Civil War as well as in Germany and the Netherlands. He focused on questions and problems with OSINT related to inferences drawn from governments; for example, studying obituaries to gauge the strength of troop numbers. But, in Block's opinion, these types of methods, based on basic empirical data analysis with a qualitative twist, may potentially raise more questions than they answer. That OSINT is seen as an increasingly popular context for data gathering (irrespective of how it is defined), even in intelligence-gathering circles, may be problematic given the increasing volume of open-source information available to governments and other institutions in an age of technological development and advancement. OSINT and the ethics of AI and digital technology application in defence policy-making will always be part of the research on AI and other digital technologies. The literature on how ethics in AI are applied will continue to grow as will the literature on OSINT's use. Alongside the challenges of ethics and OSINT, new power will continue to be applied in agile leadership in defence policy-making, and it will emerge in tandem with ongoing ethical concerns about the veracity and reliability of OSINT data.

Understanding the monumental significance of agility in the defence sector is crucial. Adaptability and swift response times are essential for maintaining a strategic edge in an ever-evolving global landscape. By prioritising agility, defence sectors can anticipate and counter emerging threats more effectively, ensuring national security and operational superiority. Regarding this, Sabben and Cros (2021, p. 1) highlight the importance of agility in defence sectors, particularly through an "agility score," which they argue is essential to achieving resilience. According to their research, "better resilience in the organisation of the defence industry requires the implementation of a new organisational model and an agile management mode, taking into account the importance of collaboration, experiential and iterative principles to be quick and responsive." This iterative, collaborative approach fosters quick decision-making and enhanced resilience, which are vital in modern military operations' fast-paced AI-driven world. They further emphasise that agility is not merely a response to change but an initiative-taking framework for fostering resilience in dynamic environments. This aligns directly with Heimans and Timms's (2018) new power model's emphasis on decentralised, inclusive, and adaptable frameworks that promote innovation and strategic flexibility.

Flournoy (2023) discusses AI's potential to "accelerate military operations, improving US forces" ability to make faster, better decisions than their adversaries.' These insights highlight the urgent need for a strategic shift toward more agile, AI-driven defence frameworks. As Flournoy suggests, "AI has sparked a security revolution—one that is just starting to unfold," making it imperative for the United States to adopt adaptable models that can quickly respond to evolving threats. The literature shows that AI is not just an emerging technology but a critical element shaping the future of warfare and defence strategy. The ability to rapidly integrate AI into decision-making processes will determine the US military's competitive edge, especially as adversaries like China continue to develop their own AI capabilities (Flournoy, 2023). The new power model, which emphasises agility, inclusivity, and real-time intelligence, is precisely the kind of adaptive framework needed to navigate the complex, high-stakes environment of modern warfare.

Burnett and Jefferson (2024) studied AI as it applies to combat and discussed its ramifications regarding both ethics and combat. The importance of agility and AI and their relationship with the new power model provide an important context for understanding both agility and the upsides and downsides of AI and ethics, as part of the discussion on agility in defence policy-making and new power. Burnett and Jefferson, in the context of technology and international studies, examined autonomous systems, specifically remote piloted vehicles (RPVs), and the expectation is that "autonomous systems will continue to increase and press in on systemic capabilities in all senses: machine-learning, AI, military R&D production, and human understanding and ingestion of new norms and tendencies" (Burnett and Jefferson, 2024, p. 198). They (p. 200) addressed an issue concerning the application of AI and new power that is not found much in the literature, and that is the discussion on AI and ethics:

> The added layer of ethical considerations must now grow commensurate to the threat of unethical and problematic usage of autonomous systems and AI given the rapidity and advancement of these systems (as in the case of RPVs, AI augmented and AI-based weapons systems and similar technological advancements for battlefield and battlespace usage).

Further, Burnett and Jefferson (2024, p. 203) focused on autonomous and AI-based systems in two case studies: the 2022 Russo-Ukraine war and the 2023 Israel-Gaza war. “As for the use of autonomous weapons systems, the 2022 Russo-Ukraine war included plenty of examples of the use of UAVs, colloquially known as “drones,” and other types of AI-influenced weaponry.” In the 2023 Israel-Gaza war, the Israelis were “attempting to snuff Hamas out of 1,300 tunnels stretching over 300 miles in Gaza. The IDF utilised AI and drones. At the same time, in December 2023, the United Nations had passed a resolution that had the support of over 150 nation-states calling into question ‘concerns’ the world body had with ‘new military tech’ and AI and ‘autonomy in weapons systems’” (Burnett and Jefferson, 2024, p. 204).

In closing, as the literature review demonstrates, integrating AI and agile frameworks is essential for enhancing the US military agility and enabling the real-time, data-driven decision-making that modern security environments demand. The new power model’s emphasis on transparency, collective intelligence, and adaptability directly aligns with the capabilities offered by AI, particularly in the context of OSINT, which will be explored in the next section. By leveraging AI-driven insights and fostering collaboration across all levels of military operations, the United States can ensure its defence strategies are responsive to current threats and proactively adaptive to future challenges. This leads us to a deeper exploration of how the new power model can drive agile decision-making in the US intelligence through the effective use of OSINT.

Applying the new power model agile decision-making for US intelligence

Open-source intelligence has become indispensable in military operations. It systematically collects, analyses, and interprets publicly available information to produce valuable intelligence (Weaver, 2017). This method has gained significant traction because it effectively addresses modern security threats and provides valuable insights to US military decision-makers and strategists. Williams and Blum (2018, pp. 1–49) discussed the evolution and importance of OSINT in the intelligence community. Their study covers the definition of OSINT, its impact on the Internet and social media, second-generation OSINT, methodology, tools, methods, challenges, and advancements. The study ends with overall conclusions, new developments, opportunities, and obstacles in open-source operations. Luttwak and Shamir (2023) argue that the creativity in IDF helped militate against bureaucratisation and top-down inefficiencies. Conversely, the innovation from a more bottom-up approach helps create changes and outcomes that serve the IDF better overall. A programme related to cybersecurity and intelligence (the “Talpiot” programme) “had a significant role in the hierarchical reversal normally required for the accomplishment of any significant military innovation” (Luttwak and Shamir, 2023, p. 52–53). The creativity of IDF was assisted by their usage of more open-source information and computer tools (Or, 2016).

Open-source intelligence is aligned with the new power model by emphasising openness, participation, and collective intelligence. It emphasises openness and accessibility as it leverages publicly available information, thereby embracing transparency (Heimans and Timms, 2018, pp. 22–23). Military decision-makers gain a comprehensive view by accessing diverse sources, such as social media, websites, and satellite imagery, as underscored by Weaver (2017). Heimans and Timms' (2018) new power model encourages openness, allowing real-time insights into adversary activities and emerging trends. OSINT relies on collaboration among researchers, analysts, and communities, enhancing collective intelligence by crowdsourcing information and complementing traditional sources (Gurney *et al.*, 2024). The US military professionals tap into OSINT communities, sharing insights and validating findings. OSINT's near-real-time data is crucial for agile decision-making, and military leaders adapt strategies based on open-source insights. OSINT's agility aligns with the new power model, empowering military effectiveness. In summary, OSINT exemplifies new power dynamics by embracing openness, collective intelligence, and agility, enhancing military decision-making in our hyper-connected world. It is mission-critical for enhancing the agility of the US national defence.

The ability to quickly adapt and react to constantly evolving threats is paramount in US military operations. OSINT is critical in furnishing up-to-the-minute information that is indispensable for making tactical decisions. By leveraging OSINT's capabilities, the US military personnel can swiftly collect and analyse data from various outlets, including social media, to better understand adversary behaviours and the emergence of new patterns or trends. *Agility and rapid adaptation*: OSINT provides near-real-time data, which is critical for quick decision-making. US military personnel swiftly collect and analyse information from diverse sources, including social media. By adapting strategies based on open-source insights, the military remains responsive to evolving threats. *Transparency and collective intelligence*: OSINT relies on openly available information and embraces transparency. Collaboration among researchers and analysts enhances collective intelligence. Military decision-makers in the United States tap into OSINT communities, validating findings and gaining diverse perspectives. In summary, OSINT exemplifies Heimans and Timms's (2018) new power dynamics by promoting agility, transparency, and collective wisdom, empowering effective US military operations while enhancing the US national defence position in our interconnected global society.

During the period of Russia's invasion of Ukraine, OSINT researchers utilised a variety of publicly available online content, including geo-located tweets, videos, and images, to effectively track and monitor the movements of Russian troops (Unver, 2018). Furthermore, Unver (2018) discusses the global concern of digital surveillance in democracies, such as Ukraine, and autocracies, such as Russia, the dilemmas surrounding it, the role of the "surveillance-industrial complex," and the challenges of regulating surveillance in a technologically advanced society. Heimans and Timms' (2018, pp. 17–18) new power model of the crowdsourced ability of civilians, as part of a newer movement of real-time OSINT intelligence, is astonishing, to say the least. Through in-depth analysis of social media data, researchers could discern the gradual buildup and positioning of Russian forces along several border areas, providing crucial and actionable intelligence. This reflects the core of US strategic partnership with Ukraine regarding its defence agility. Hence, it is beneficial for US national security for its allies and partners to incorporate the Heimans and Timms (2018, pp. 14–32) new power model.

Riehle (2024) highlights how the war in Ukraine has shifted Russian intelligence activities towards more tactical targets, especially inside Ukraine. There has been a decline in the quantity of Russian intelligence activities due to the expulsion of Russian intelligence personnel from embassies across Europe. In this regard, Riehle (2024) makes the case that Russian intelligence services have been focusing on operational and tactical targets, particularly in preparation for the military campaign in Ukraine. Riehle's (2024) article analyses publicly available reports of investigations and arrests of Russian intelligence operatives, providing insight into the shift towards a more tactical focus. *Something to consider*: Although Russia is an adversary of the United States, one solution to this tactical focus could be implementing Heimans and Timms's (2018) new power model and applying it to their OSINT capabilities. This agile knowledge could be applied by the United States concerning national security. The United States may face a similar tactical situation where the agility and flexibility of leveraging crowdsourced intelligence could save the lives of civilians and warfighters in a future conflict.

A swift aggregation and comprehensive analysis of open-source information enabled timely and informed decision-making, contributing significantly to situational awareness during a critical international event (Popescu and Carpen, 2024). Moreover, OSINT plays a crucial role in facilitating the exchange of information and cooperation among researchers. It underscores the value of utilising crowdsourced data to improve intelligence (Gurney *et al.*, 2024). The US military experts can use OSINT networks to exchange knowledge, validate discoveries, and access varied viewpoints. The combined endeavours of the OSINT community complement conventional intelligence outlets, thereby improving US military national defence capabilities. The emerging new power model by Heimans and Timms (2018) aligns with OSINT in several ways, including decentralisation and democratisation of information, crowdsourced intelligence and collective sense-making, agility and timeliness, transparency and accountability, and human–AI collaboration. These connections highlight how OSINT's approach aligns well with the evolving power dynamics introduced by Heimans and Timms (2018) in our interconnected world, enhancing situational awareness, decision-making, and US national defence during critical events.

In summary, integrating the principles of OSINT and utilising its associated tools can profoundly enhance the US military's agility, situational awareness, and decision-making capabilities for national defence. By fostering a culture of transparency, inclusivity, and collaborative knowledge-sharing, the US military professionals can effectively navigate the complexities of an interconnected world and strategically respond to the constantly evolving global environment (Thompson *et al.*, 2024). OSINT's decentralised, transparent, and collaborative approach resonates with the principles of the new power model, enabling effective responses in an interconnected world (Heimans and Timms, 2018).

Conclusions

This article has argued that OSINT will have a major influence on the future of US defence strategies and policy. It is apparent that OSINT is very transparent and collaborative, in terms of information and technology, in allowing American military leaders and policymakers to improve tactical and strategic decisions. It is our contention that the work of Heimans and Timms (2018) on new power allows leaders and organisations to conceptualise both informational and social media platforms in ways that emphasise and augment agility, transparency, crowdsourcing, technology, and other information and information-related imperatives that can assist and ameliorate basic tactical and strategic thinking and applications in the defence and policy-making communities. As we see in militaries, like the IDF, which has an OSINT unit—known as Hatzav—the use of OSINT, and creative approaches to decision-making and conceptualisation of problems and issues, have led to improved outcomes and efficiencies in military administration, war-making, and R&D (Luttwak and Shamir, 2023, p. 219). The same could be said for the United States, with a greater application of new power ideals, as increased new media and technologies (including AI) begin to impact the modes of operation in Washington.

This article discussed the literature related to OSINT, AI, and its relationship with Heimans and Timms's (2018) new power model. The potential for agile decision-making and leadership in the American defence policy-making space continues to evolve in accordance with Heimans and Timms's conceptualisations, which allow leaders and policymakers to make decisions in real-time and utilise OSINT in ways that improve the quality of information, the quality of discussions that inform defence policy-making, and the production of defence-related products and decisions. Thus, the importance of this article to the literature will continue to manifest as technology and AI are used increasingly in defence work and applications during training and on the battlefield (Burnett and Jefferson, 2024). Further research into how the new power model is understood, works, and is applied in defence and security studies in Western democracies will assist in building increased openness and scholarship in the field. More focus on open-sourced innovation (as per the IDF model) in the defence sector, on new power as a concept, and on processes and decision-making informed by OSINT is required to advance the literature in this area of defence and security studies. The article's limitation is tied to the lack of literature on the new power model and its application to the use of OSINT and agile leadership in the context of American defence system and policy-making apparatus. This has not been done before and the literature on new power (as conceptualised by Heimans and Timms, 2018) is not deep or wide. However, other works by students of leadership and global affairs, such as Naim (2013, pp. 1–14), and students of leadership and organisational change, such as Johansen (2017), that focus on the end of traditional conceptualisations of power and leadership may help us understand better how new power can be understood in organisational life and processes in many Western policy-making bodies, such as the US Defence Department.

Funding

This research received no external funding.

Author Contributions

Conceptualisation, methodology: K.W.J., S.R.W.; validation: S.R.W.; formal analysis, investigation: K.W.F., S.R.W.; data curation: S.R.W.; writing – original draft preparation, writing – review: K.W. J., S.R.W.; visualisation, supervision, project administration: K.W. J.

Data Availability Statement

Not applicable.

Disclosure Statement

No potential conflict of interest was reported by the authors. The authors read and agreed to the published version of the manuscript.

References

Baker, J.E. (2024) 'Practicing at the speed of relevance: emerging technologies and the emerging nature of natural security law,' in Gibson, T.T. and Jefferson, K.W. (eds.) *International security studies and technology: Approaches, assessments, and frontiers*. Northampton, MA: Edward Elgar Publishing, pp. 76–99.

Block, L. (2023) 'The long history of OSINT', *Journal of Intelligence History*, 23(2), pp. 95–109. doi: 10.1080/16161262.2023.2224091.

Burnett, R.E. and Jefferson, K.W. (2024) 'Autonomous systems applications in weaponry and intelligence, surveillance, and reconnaissance: ethics and conflict', in Gibson, T.T. and Jefferson, K.W. (eds.) *International security studies and technology: Approaches, assessments, and frontiers*. Northampton, MA: Edward Elgar Publishing, pp. 196–207.

Department of Defense (2023) *Data, analytics, and artificial intelligence adoption strategy: Accelerating decision advantage*. Available at: https://media.defense.gov/2023/Nov/02/2003333300/-1/-1/1/DOD_DATA_ANALYTICS_AI_ADOPTION_STRATEGY.PDF (Accessed: 23 October 2024).

Flournoy, M.A. (2023) 'AI is already at war: How artificial intelligence will transform the military', *Foreign Affairs*, 102, p. 56.

Gibson, T.T. and Jefferson, K.W. (eds.). (2022) *Contextualizing security: A reader*. Athens, GA: University of Georgia Press.

Gurney, N., Morstatter, F., Pynadath, D.V., Russell, A. and Satyukov, G. (2024) 'Operational collective intelligence of humans and machines', in Hirohiko, M. and Ymi, A. (eds.) *International conference on human-computer interaction*. Cham: Springer Nature, pp. 296–308.

Heimans, J. and Timms, H. (2018) *New power: How power works in our hyperconnected world—and how to make it work for you*. New York, NY: Doubleday.

Henrekson, M. and Stenkula, M. (2024) 'Bottom-up policies trump top-down missions', in Henrekson, M., Sandström, C. and Stenkula, M. (eds.) *Moonshots and the new industrial policy: Questioning the mission economy*, vol. 56. Cham: Springer, pp. 309–331. doi: 10.1007/978-3-031-49196-2_17.

Jefferson, K.W., Mather, R.D., Bennet, J., Cairo, III, L., Harbolt, L., Ratterman, P.M., Sherrod, J., Story, S., Sturtzel, N., Teater, J. and Thomas, C. (2021) 'New power through the lenses of leadership studies, psychology, and politics', *Journal of Scientific Psychology*, 17 (February), pp. 1–10.

Johansen, B. (2017) *The new leadership literacies: Thriving in a future of extreme disruption and distributed everything*. Oakland, CA: Berrett-Koehler Publishers.

Khorram-Manesh, A., Mortelmans, L.J., Robinson, Y., Burkle, F.M. and Goniewicz, K. (2022) 'Civilian-military collaboration before and during Covid-19 pandemic—A systematic review and a pilot survey among practitioners', *Sustainability*, 14(2), p. 624. doi: 10.3390/su14020624.

Klaus, L.C.O. (2016) 'Transforming armed forces through military transparency: Open government challenges in a world of secrecy', *Transforming Government: People, Process and Policy*, 10(1), pp. 99–119. doi: 10.1108/TG-01-2015-0002.

Luttwak, E.N. and Shamir, E. (2023) *The art of military innovation: Lessons from the Israel defense forces*. Cambridge, MA: Harvard University Press.

Marwala, T. (2023) 'Militarization of AI has severe implications for global security and warfare', UNU. Available at: https://unu.edu/article/militarization-ai-has-severe-implications-global-security-and-warfare (Accessed: 23 October 2024).

Mikhailov, D.I. (2023) 'Optimizing national security strategies through LLM-driven artificial intelligence integration', *arXiv preprint arXiv:2305.13927*. doi: 10.48550/arXiv.2305.13927.

Moreno, J., Gross, M.L., Becker, J., Hereth, B., Shortland, III, N.D. and Evans, N.G. (2022) 'The ethics of AI-assisted warfighter enhancement research and experimentation: Historical perspectives and ethical challenges', *Frontiers in Big Data*, 5. Available at: https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2022.978734/full (Accessed: 23 October 2024).

Naim, M. (2013) *The end of power: From boardrooms to battlefields and churches and states, why being in charge isn't what it used to be*. New York, NY: Basic Books.

Or, C. (2016) *Open source culture: To what extent has the defense establishment adapted to software culture, and what does it say about its level of innovation?* Jerusalem: Dado Center (IDF). Available at: https://www.idf.il/en/mini-sites/dado-center/vol-7-force-design-b/open-source-culture/ (Accessed: 23 October 2024).

Popescu, G. and Carpen, S. (2024) 'The rise of open-source intelligence in the Russia-Ukraine war', in Dan-Suteu, S., et al (ed.) *Proceedings of the International Scientific Conference Strategies xxi*, vol. 19. Frankfurt am Main: Central and Eastern European Online Library (CEEOL), pp. 142–148.

Proctor, S. and Daniels, C.B. (2020) 'Implementing agile project management in the US Department of Defense', *Space Infrastructures: From Risk to Resilience Governance*, 57, p. 337.

Rasmussen, M.F. (2012) *A framework of organizational empowerment for strategic military leaders.* Carlisle, PA: US Army War College. Available at: https://apps.dtic.mil/sti/pdfs/ADA561792.pdf (Accessed: 23 October 2024).

Riehle, K. (2024) 'The Ukraine war and the shift in Russian intelligence priorities', *Intelligence and National Security*, 39(3), pp. 458–474. doi: 10.1080/02684527.2024.2322807.

Rowe, N.C. (2022) 'The comparative ethics of artificial-intelligence methods for military applications', *Frontiers in Big Data*, 5. Available at: https://www.frontiersin.org/journals/big-data/articles/10.3389/fdata.2022.991759/full (Accessed: 23 October 2024).

Sabben, N. and Cros, S. (2021) 'Use an agility score to be more resilient: The defense sector', American Society of Public Administration (ASPA). Available at: https://hal.science/hal-03221296/ (Accessed: 23 October 2024).

Thompson, E., Jorstad, A., Nemr, C. and Corwin, B. (2024) 'Collaboratorium: A multi-stakeholder approach to advancing innovative defense acquisition', in *Proceedings of the twenty-first annual acquisition research symposium.* Acquisition Research Program; Monterey, CA: Naval Postgraduate School, pp. 73–93.

Unver, A. (2018) *Digital open source intelligence and international security: A primer.* EDAM Research Reports, Cyber Governance and Digital Democracy, No. 8. SSRN paper series. Rochester, NY: SSRN-Elsevier. Available at: https://ssrn.com/abstract=3331638 (Accessed: 23 October 2024).

Weaver, G.S. (2017) 'The police and the military: Future challenges and opportunities in public safety', in *Open source intelligence (OSINT)*, O'Dea, M. and Jarvis, J. (eds.) *Proceedings of the futures working group,* vol. 4. Orlando, FL: Futures Working Group (FWG), University of Central Florida.

Williams, H.J. and Blum, I. (2018) *Defining second generation open source intelligence (OSINT) for the defense enterprise*. Santa Monica, CA: Rand Corporation.