ACIG
APPLIED CYBERSECURITY & INTERNET GOVERNANCE

NASK

Examining Supply Chain Risks in Autonomous Weapon Systems and Artificial Intelligence

Austin Wyatt | RAND Australia, ORCID: 0000-0003-1901-8019

Received: 7.06.2023

Accepted: 17.11.2023

Published: 29.11.2023

Cite this article as:
A. Wyatt "Examining Supply Chain Risks in Autonomous weapon systems and Artificial Intelligence," ACIG, vol. 2, no. 1, 2023, DOI: 10.60097/ACIG/162874

Corresponding author:
Austin Wyatt, RAND Australia; ORCID: 0000-0003-1901-8019;
E-MAIL: awyatt@rand.org

Abstract

The development of increasingly AI-enabled autonomous systems and other military applications of Artificial Intelligence (AI) have been recognised as emergent major military innovations. In the absence of an effective and enforceable ban on their development and/or usage arising from the Group of Governmental Experts on Lethal Autonomous Weapon Systems (LAWS), it is likely that such systems will continue to be development. Amongst the legal, ethical, practical, and strategic concerns raised by the emergence of such systems, it is important not to lose sight of the risks involved in relying on a high-manufactured system in place of a human. This places additional strains and importance on securing diverse, complex, and over cross-jurisdictional supply chains. This article focuses on the vulnerability of and the risks to the integrity and security of the supply chains responsible for producing AI-enabled autonomous military systems.

Keywords

supply chain risk, autonomous weapon systems, Artificial Intelligence, emerging technology

1. Introduction

The increasing and continuous development of autonomous systems and other military applications of that consist of and/or include Artificial Intelligence (AI) have been recognised as an emergent major military innovation [1]. This recognition is underscored in strategic documentation from both China [2] and the United States [1], along with attendant large-scale investments from both state and commercial actors. Recognition of AI as an emergent major military innovation in the US and China is particularly important because they are locked in hegemonic competition in the Asia Pacific and account for the vast majority of military expenditure, both in terms of procurement and research and development. Amongst the benefits advanced in support of developing AI-enabled autonomous systems, their potential to safeguard soldiers by removing them from the direct line of fire is commonly cited. Another benefit is that AI-enabled systems confer a strategic advantage by facilitating tactical and operational decision making at a pace exceeding human capability. Even if one assumes that these benefits are achieved, such systems also raise numerous ethical and legal issues [1], as well as arguably increasing risk to non-combatants [3] – commonly referred to as collateral damage. Whether autonomous systems will be a net positive or negative influence on the future of warfare ethics, in the absence of significant advances in the efforts at the Convention on Certain Conventional Weapons [1] toward an international legal ban,[1] they are likely to remain prominent in the future paradigm of conflict, and thus have significant impact on the achievement national security objectives.

It is therefore important that the international community considers the viability and attendant risks involved in relying on military applications of AI, including AI-enabled autonomous weapon systems. AI is best thought of as an enabling innovation, closer to electricity than the machine gun [50], and is the core component of any autonomous systems. Part of the challenge in doing so is the lack of a universally agreed set of terminology for engaging in the debate around responsible use of AI in the military domain[2], (beyond that they are generally non-deterministic complex systems without an integrated human operator. Even lethal autonomous weapon systems, arguably the most problematic AI-enabled military technology category, lack a universal definition [1]. While most writers start with the definition presented by US Directive 3000.09 [4][3], other definitions abound including from the UK Ministry of Defence [5], and the Australian Defence Force [6], as well as from academia include those published by Horowitz [7], Scharre [8], Roff [9], Wyatt [1], and Bode, Huelss and Nadibaidze [10].

1 The United Nations Convention on Certain Conventional Weapons (CCW) has held semi-annual meetings of selected governmental experts on Lethal Autonomous Weapon Systems since 2014. These meetings were part of an effort to develop international legal instruments for governing the use of AI-enabled autonomous weapon systems and was the main arena in which a pre-emptive ban was mooted. Although its consensus-based approach has not yet yielded conclusive results, it did support the passing of the first General Assembly resolution on autonomous weapons in 2023.

In the absence of a universally agreed definition for AI-enabled autonomous systems, it has become increasingly commonplace to leverage the three functional autonomy categories developed by the International Committee of the Red Cross and Human Rights Watch. This approach categorises systems are categorised by their ability to execute its 'critical functions' independent of a human operator [11]. An AI-enabled system could, therefore, be described as a supervised autonomous systems (where a human remains on the decision loop, where they can interrupt the system's actions), semi-autonomous systems (where the system has a limited capability to act autonomously within geographic or functional limitations, and a human remains in the decision loop), and fully autonomous systems (where the system has effectively independent control of its critical functions, removing the human from the decision loop) [1].

The absence of a human operator places even more emphasis on the reliability and effectiveness of the system itself. A sufficient level of certainty and safety inherent in these systems is not merely contingent on the technology maturing to a set future point [12]. Instead, one must take a more holistic approach, one that considers other elements and actors that may influence or compromise the effectiveness and reliability of future AI-enabled autonomous weapon systems, whether due to error or malicious action.

This article focuses on exploring the risks associated with the integrity and security of the supply chains responsible for producing AI-enabled autonomous systems. Supply chains are, by their nature, complex networks with multiple nodes and links, each vulnerable to potential disruptions and security breaches [13]. Such networks typically span geographic and jurisdictional boundaries and are reliant on many of the same key transit points as more general global trade. The dislocated nature of the global supply chain for AI-related technologies and the wide range of civilian as well as military actors increases the complexity of securing accountability [56]. Disruptions to critical technology supply chains, such as those associated with the military industrial complex and associated national security operations, could delay or prevent the deployment and maintenance of AI-enabled autonomous systems during times of increased competition or conflict. Fedasiuk et. al. highlight the potential for an adversary to hamper western access to crucial advanced chip sets [57], a risk that is particularly concerning given the vulnerability of the main supplier of such chips, Taiwan, to China. Uniquely to AI-enabled systems, there are also risks involved in the supply chains for the data that make these systems intelligent. Morgan et. al. suggest that even air-gapped AI-enabled systems, while more resilient against hacking,

3 — "A weapon system that, once activated, can select and engage targets without further intervention by an operator. This includes, but is not limited to, operator-supervised autonomous weapon systems that are designed to allow operators to override operation of the weapon system, but can select and engage targets without further operator input after activation" [4].

remain vulnerable to degradation through data poisoning attacks, where an adversary maliciously injects code into the training data to fool the resultant system, or via physical adversarial attacks, such as specially designed stickers that fool computer vision algorithms [58]. Resilience must be built early into supply chains to ensure that such systems are not compromised by contamination of their training data or the insertion of zero-day exploits [14][4].

Given the breadth of AI-related risks in logistics, this article limits itself to exploring the supply chain risks that could stem from adopting AI and AI-enabled autonomous systems. This paper is also intended to provide a broad introduction to the issues, a further exploration of these issues from the perspective of particular military or regional perspective.

2. AI, Autonomous Systems and Future of Conflict

The rise of AI-enabled Autonomous Weapon Systems (AWS) as a potential Revolution in Military Affairs (RMA) is anticipated to have a revolutionary, and thus as disruptive impact on the future of conflict. Despite popular belief, innovation requires both the maturation of an invention and the development of operational concepts to utilise that invention in a disruptive manner [15]. This does not merely represent a pioneering deployment of an autonomous system by a state; instead, different states might opt for unique development strategies for related technologies or pair a matured autonomous system with distinct yet non-revolutionary operational concepts [15]. Moreover, developers may adopt strategies to limit the exposure of their methods to safeguard operational advantage or to avoid international scrutiny, particularly in the case of LAWS [16]. Eventually, a state will introduce a fully autonomous weapon system that disrupts conventional military balances,[5] compelling other states to react to the resultant shift in relative power [17] or relative advantage. This pivotal moment, known as the demonstration point, obliges competitor states to respond or concede strategic advantage to the initial state deploying such systems [15].

However, first mover advantage may be transient, particularly when it pertains to disruptive innovations like AI-enabled autonomous systems, hypothesized to possess low proliferation barriers [1]. Past military innovations typically demanded considerable resources or organizational capital, limiting the ability of states to respond to a demonstration point by matching the initial mover's advancements.

4 — Zero day exploits are vulnerabilities in a computer system that are unknown to the users or manufacturers until they are deployed by an adversary. These are particularly concerning in the case of AI-enabled systems because of the complex nature of such systems. This risk is further exacerbated by the vulnerability of AI to corruption (whether deliberate or not) of the underlying training data set.

5 — This refers to the relative capacity of states to "adopt the key military methods of a period" [15], which in the current paradigm could include precision munitions, space-based communications, and aircraft carriers.

When faced with novel forms of warfare, for example, the advent of aircraft carrier warfare, a less powerful state theoretically could attempt to surpass the first mover, but practical constraints of resources and political will would limit this [15]. The adaptation/adoption of doctrine, not a trivial matter, also needs consideration. Yet, if the barriers for entry and early adoption are significantly diminished (due to the dual-use nature of related technologies or lack of need for specialized skill sets), the disruptive effects of rapid proliferation to multiple state and potentially non-state actors should be considered [18], as exemplified by the widespread use of remotely operated armed drones [19]. Such proliferation would also have a significant impact on supply chain vulnerability once these technologies become widely distributed.

Predicting the precise effects of such proliferation on future warfare remains challenging. However, historical insights from military and civilian disruptive innovation theory, such as aircraft carrier warfare [15], coupled with the unique attributes of LAWS (and other AI-enabled military technologies), as well as initial state reactions to their early development, provide a first-order, yet robust foundation for hypothesizing potential outcomes. An overarching characteristic of major military innovations is their transformative influence on how states project power and conduct warfare [1]. Historically, this has precipitated disruptions in the international balance of power, providing opportunities for middle and minor power states to challenge existing hegemonic power balances, in both global and regional contexts. This change can enable a rising challenger state (such as China) to counterbalance the traditional advantage enjoyed by the existing hegemon (in this case the US), while smaller states strive to mimic successful states (e.g. Taiwan mimicking the US) to safeguard their own power bases from their rivals, thereby accelerating diffusion [20]. Threatened by the deterioration of its relative advantage, the incumbent state is induced to adopt or enhance the tempo of its Revolution in Military Affairs (RMA) efforts to regain its standing [1]. This diffusion of major military innovation may engender regional instability and precipitate hegemonic warfare [21] – typically referred to an arms race or a negative security cycle within the realist paradigm. Given the relatively low adoption barriers for autonomous weapon systems compared to prior major military innovations like nuclear weapons, and the comparative difficulty in applying conventional arms control mechanisms [51], it is hypothesized that the emergence of LAWS will have a destabilizing influence on the future of warfare.

From a grand strategic standpoint, the potential for middle and minor powers to emerge as successful early adopters of AI-enabled

autonomous systems represents a departure from historical precedents, like nuclear weapons, where middle and minor powers were compelled to align with a great power competitor to protect their interests [2]. Instead, states in the global South could potentially exercise greater autonomy, balancing competing great powers regionally while deterring aggression from similarly sized neighbours. This could instigate an escalating cycle of arms acquisition and posturing as regional powers deploy systems lacking effective legal or normative controls, thus intensifying security dilemmas [20]. Without mutually accepted norms around appropriate uses and responses to such systems or effective international legal treaty banning their use (for example through the CCW), there is a considerable risk of unanticipated escalation, whether between the great powers or between regional powers in Southeast Asia or Africa for example. Additionally, the spread of remotely operated, autonomous, and/or AI-enabled systems, especially given the dual-use nature of enabling technologies, poses a significant risk of these systems falling into the hands of violent non-state actors. The result may be a less stable balance of power, particularly in the Asia-Pacific, leading to a multipolar military competition domain rather than a traditional hegemonic transition of power.

While considering the influence of these systems on regional stability and the likelihood of new conflict or the prolonging of existing conflict, it is important to debunk two persistent myths surrounding AI-enabled autonomous weapon systems. The first is the fear of a 'Terminator' being developed or deployed in the foreseeable future.[6] Designers and potential state end-users are rational actors who are generally cognizant of the ethical issues raised by LAWS.[7] Admittedly, this would not apply to violent non-state actors such as terrorist groups or extremist individuals. Secondly, the rise of AI-enabled autonomous weapon systems does not signify that future wars will become 'bloodless' or 'sterile' [25]. War remains a human endeavour, and human casualties, particularly among civilian populations in urban operations, are unfortunately inevitable – be it intentional or collateral. Both of these perspectives oversimplify the issue, disregarding the more plausible scenario of widespread deployment of these systems disproportionately affecting the technologically inferior adversaries [26]. The introduction of autonomous systems raises significant ethical challenges, particularly regarding the kill-decisions [3]. Simultaneously, there is a moral obligation on leaders to utilize autonomous systems where they can protect the lives of soldiers, even if their deployment is limited to the dull, dirty, and dangerous roles [27]. With all this said, it would now be pertinent to consider the vulnerability of supply chains as single points of failure for the security of these systems.

6 —— For example the discussion by Shead and the concept of 'slaughterbots' [22].

7 —— While this is a broad claim, it is supported by perception studies focused on Machine Learning developers [23] and ADF personnel [24], as well as the recent call from Open AI's CEO for greater regulation of the area.

3. Supply Chain Risks

Increased reliance on AI-enabled systems also increases the variety and seriousness of vulnerabilities in the supply chain. AI-enabled Autonomous systems would not be reliant on a human for critical functions [10]. In addition to the myriad legal and ethical challenges this change poses, however, it also quite simply places the entirety of the burden for that system to run effectively, reliably, and safely on manufactured components. There is no human to recognise and correct errors; for example, that the scope of a rifle was incorrectly zeroed or that a civilian aircraft has been mis-identified as a legitimate target. Ensuring that AI-enabled systems operate as expected and fail safely thus become crucial characteristics, yet they are dependent on securing disparate and often complex trans-regional and trans-national supply chains. In the following section, key geo-strategic-, technological-, and economic risks to these chains will be examined.

3.1. Geostrategic Supply Chain Risks

Beginning with the geostrategic risks associated with the supply chains for AI-enabled systems sensibly reflects the recognition of the likely importance of such systems to the future of warfare. Further, even amongst states that do not see themselves as a potential first mover, the strong public commitment to AI and autonomy by the US and China encourage smaller states and violent non-state actors to invest in mechanisms for countering the advantage offered by such systems, with the supply chain being a novel and comparatively vulnerable attack surface.

First, despite the recent surge in public accessibility of Large Language Models, machine-learning based complex AI remains expensive [28] and reliant on large amounts of computing power [29], cooling [30], and above all, data (which raises its own ethical and legal challenges) [31]. Reliance on a global supply chain diminishes the capacity of states from a sovereign control perspective, particularly non-great powers, to guarantee access and to impose sufficient security controls over the manufacturing and development process. For example, rare earth metals, crucial for many advanced technologies, are primarily sourced from a few countries, presenting a geopolitical risk if these countries decide to leverage their monopolistic control over these resources. In the event of geopolitical tensions, a trade war or even an embargo, their access to critical resources may be limited. A case in point would be a blockade of Taiwan could have immediate and disastrous effects on high-technology supply chains internationally [32]. **The current sanction regime against Russia**

due to the illegal war with Ukraine provide ample real-time examples of how military industrial complex and dual-use supply chains affect the ability of even a superpower to maintain (relative) advantage.[8]

Relatedly, and of particular concern for states such as Australia, international technological controls and regulations can impact the availability and transfer of technology, particularly for emergent or particularly sensitive systems. International Traffic in Arms Regulations (ITAR) is a particularly well-known example of how countries may restrict the export of technologies deemed either critical to national security or related to maintaining a particular capability advantage [33]. Additionally, international regulatory bodies – for example the Wasserman Arrangement – of which Australia is a signatory nation amongst 44 other nations[9] – may impose restrictions or sanctions on AI and autonomous system-related technologies or developers. For example, the international community continues to debate whether a ban on autonomous weapon systems is appropriate, or likely to be effective. Supply of critical components could be limited or blocked if such a ban were implemented, or if individual states or a bloc – such as the EU – were to implement their own restrictions. This risk would be particularly troubling if AI or autonomous weapon systems come to rely on a single source for a critical component, such as high-capability semi-conductors produced primarily in Taiwan. Such dependency creates a strategic vulnerability because any disruption to the supply from this source – due to logistical issues, manufacturing constraints, or other factors – can result in severe manufacturing and subsequent operational setbacks – severely affecting the ability to secure national interests. It also gives the supplier considerable leverage, potentially leading to increased prices, unfavourable terms and/or even insisting on being included into economic/defence pacts such as NATO or the Five Eyes Alliance.

Contrastingly, a diversified, multi-jurisdictional supply chain increases the risk of intellectual property (IP) theft or duplication, as well as the potential for proliferation of such systems to smaller states and violent non-state actors. The development and application of AI in military contexts often involve proprietary algorithms, data models, and technologies, representing substantial intellectual capital. This sensitive information, if leaked or stolen, could significantly undermine a nation's technological edge and compromise its national security. Supply chains that span across multiple countries and vendors increase the risk of such IP being compromised, especially if these entities have differing or inadequate cybersecurity measures and

8 —— The author would like to thank Dr Dries Putter for this example.

9 —— The author would like to thank Dr Dries Putter for suggesting the Wasserman Arrangement as an example.

different levels of security consciousness. Consequently, it becomes crucial to ensure robust protection of IP across the entirety of the supply chain [13] which will require significant counterintelligence measures and thus increasing the unit costs concomitantly. In the absence of such protections, there is also a risk of uncontrolled proliferation, exacerbated by the dual-use nature of the underlying technologies. The risk of such systems falling into the hands of adversarial or rogue states, non-state actors, or even terrorist groups is a significant security risk that's mitigation is complicated by cross-jurisdictional supply chains involving multiple civilian actors. This technology proliferation can lead to an advantage leveling effect on the strategic landscape, increased risk and severity of extremist/terrorist violence, and could raise the security vulnerability for states that would not otherwise vigorously pursue such weapons.

Finally, given the importance publicly placed on AI by leading militaries (such as the United States, China, and Russia), one must also consider the risk of a malicious non-state actor (whether a disgruntled insider threat, terrorist group or extremist) deliberately interfering with, disrupting, delaying or degrading critical supply chains, reducing or eliminating the capacity of a state to produce and maintain key military systems [34]. The principal risk surfaces for this are arguably in the cyber domain, particularly in the face of US decoupling and friend-shoring efforts. A key mechanism for this sort of malicious action is through the cyber domain. The low entry cost of operations in the cyber domain (whether attack, subversion, or intrusion) encourages their use by smaller actors, particularly those utilising existing AI tools as force-multipliers. For such actors, the opportunity to disrupt or sabotage high-capability high-cost systems through exploiting vulnerabilities in their supply chains, is an attractive levelling mechanism. Such attacks range from the theft of critical intellectual property [13] to the malicious manipulation of training data [35]. The high level of interconnectivity in global supply chains, as demonstrated by Covid-19, and the widespread use of digital systems in both official tasks and in the homes of related individuals exacerbate these risks [36]. Even onshoring sufficient manufacturing capabilities to produce key components domestically does not eliminate these risks, as interdiction could be launched lower down in the supply chain, at the raw materials level, for example [34].

3.2. Technological Supply Chain Risks

The first technological supply chain risk pertains to technology obsolescence. Given the rapidity of technological development in the field of AI, there is a substantial risk that any procured

technology may become obsolete soon after acquisition. This fast-paced evolution is fuelled by constant advancements in algorithms, data processing capabilities, and computational hardware – fuelling the RMA concept internationally. The implications of technological obsolescence are multifaceted and significant. First, the financial resources invested into the design, manufacturing, acquisition, integration, and training of personnel for specific AI technologies could become sunk costs if these technologies rapidly become outdated. This risk is exacerbated by the typically protracted defence procurement processes, which often lag behind the pace of technological advancements. The discrepancy in pace between procurement and technological progress could result in the acquisition of technologies that are already verging on obsolescence at the point of implementation. Operationally, the consequences could be equally detrimental. Outdated AI technologies could impair a military force's effectiveness, potentially leading to tactical and strategic disadvantages in the field. Moreover, support for older technologies may diminish as manufacturers and software developers move towards more advanced and efficient models, making it difficult to maintain and repair existing systems. Lastly, as AI technologies continue to evolve and proliferate globally, maintaining up-to-date systems is paramount as operating outdated systems could expose vulnerabilities to potential adversaries and compromise the security and effectiveness of military operations and thus national security. The need to avoid obsolescence in not only the end product but the key production nodes for such systems makes it imperative for militaries and manufactures to adopt an agile approach to technology acquisition and implementation. This could involve shortening procurement cycles, investing in regular technology refreshment programs, and establishing collaborative partnerships with technology providers to ensure early access to cutting-edge AI technologies [37]. Additionally, incorporating flexibility in procurement contracts to accommodate technological upgrades can also help in keeping pace with rapid advancements [38]. Of course, it has to be said that increasing the tempo of technology uptake in organisations will also open the vulnerabilities to increased levels of corruption and graft typically associated with defence contracting – and hence the long and bureaucratic procurement processes to ensure transparency and accountability. Thus, corruption due to the requirements for agility within supply chains poses another distinct challenge to security.[10]

The second major risk involves the complexity and fragmentation of supply chains inherent in the production and deployment of AI technologies. These supply chains often stretch across the globe,

10 —— The author would like to thank Dr Dries Putter for this point.

involving various suppliers for essential hardware components, software applications, and data resources. This complexity and fragmentation engender a multitude of risks. For one, a disruption at any point in the supply chain, whether it's a failure to produce a critical hardware component, a disruption in logistical operations, or a software development issue, can have a significant downstream effect. This can potentially delay or even halt the delivery and deployment of AI technologies, severely affecting the military's operational readiness and capabilities. The fragmentation of the supply chain also raises issues regarding quality control and security. With multiple suppliers involved in the production process, maintaining consistent quality standards across all components becomes challenging. This was illustrated repeatedly with the security challenges faced by the F-35 development and production efforts [39]. Similarly, with so many points of entry in the supply chain, the risk of malicious actors introducing vulnerabilities into the system is significant. Mitigating these challenges could take the form of friend-shoring, supporting the development of alternative suppliers of key components and raw materials in allied states in order to reduce the threat surface [40], or implementing (contractually or through legislative tools) strong quality control and cybersecurity protocols across key nodes of the supply chain. However, these issues aside, there is also good reason for having fragmented supply chains – i.e. fragmented insight into the total composition of a sensitive system. Thus, there needs to be a balance between the requirements for supply chain fragmentation and the need to security.

The third technological risk relates to the potential vulnerabilities of AI systems themselves. These could be due to design flaws, manufacturing defects, malicious interference, or software code malfunctions [14]. Unfortunately, due to the tendency of such complex systems to fail, the results of such vulnerabilities in a military context could be severe, and would damage vital trust between the system and its human user/supervisors even if the malfunction does not cause physical harm. Such trust is a integral part of technology adoption by the organisation to the point where doctrine is written for it or adapted to accommodate it. This risk is exacerbated by the opaqueness nature of certain AI systems, the so called black-box problem [41]. The lack of transparency, explainability, and common understanding of an AI-system's functionality makes it difficult to predict and understand system behaviour, especially in emergent situations [42], for example the recently disclosed thought experiment in which an AI system operating in a simulated environment eliminated its (simulated) human overseer in order to maximise its capacity to fulfil its core mission [52].

Cybersecurity threats represent a further significant concern. As digital systems, AI technologies are attractive targets for cyberattacks that could degrade or disable them in store or on the battlefield [14]. The source of these cyber threats could range from state-sponsored actors aiming to disrupt military capability, to violent non-state actors such as terrorist groups or organized crime syndicates seeking to exploit vulnerabilities for their own ends. Importantly, these vulnerabilities could be introduced at any stage of the supply chain, underscoring the necessity of end-to-end security measures – with concomitant cost implications for the end user.

3.3. Economic Supply Chain Risks

Another salient aspect in the discourse on the adoption of AI by militaries is the substantial expenditure associated with the development, deployment, and maintenance of these advanced systems. It is an inherently resource-intensive pursuit, requiring considerable investment in various facets of the development and procurement processes. The research and development phase, the cornerstone of AI evolution, demands a prodigious financial commitment and human capital outlay [43]. Furthermore, recruiting and retaining skilled personnel capable of undertaking such complex development tasks also represents a significant financial undertaking, especially considering the high demand for these experts in the competitive technology market [44] and the further cost of security vetting and maintaining security from an insider threat perspective – the Edward Snowden incident being a case in point. Access to the best-quality (highly qualified and/or experienced doctoral qualified researchers) specialist talent, including data scientists and machine learning experts, is pivotal to driving innovation and improving the operational efficiency and reliability of military AI applications [12]. For example, acquiring top-level talent is a known barrier in Chinese military AI efforts, due to government policies and the opportunities offered by working in the US or Europe [2]. Once an AI system is developed, the procurement process entails substantial funding [44]. The hardware, comprising high-speed processors and robust storage solutions, forms the backbone of AI capabilities. Simultaneously, software and data acquisition are critical for the system's decision-making ability, as it feeds and trains the underlying algorithms. Additionally, AI technologies require ongoing updates and maintenance, further escalating the overall costs. This continued investment is essential to keep abreast of rapid technological advancements, ensure system security, and mitigate potential obsolescence. These updates may encompass software patches to enhance the system's capabilities or address vulnerabilities, hardware upgrades to improve performance,

and data management activities to ensure integrity and compliance with regulations. Given the high costs involved in being the first mover for AI systems, reliance on AI in military applications poses potential risks to defence budgets. There is a plausible concern that the financial burden of attempting to maintain a capability offset based solely on technological advantaged derived from advanced AI capabilities may strain defence budgets. Such arguments must be balanced against the argument that autonomous systems and other uses of military AI offer significant potential dividends in terms of enhanced operational efficiency, precision in decision-making, and maintenance costs over their life of type. While initial costs are generally exorbitant (and hence also resulting in very high entry barriers for competitors), AI systems have proven to be far cheaper to duplicate and diffuse once in use, meaning that the bar to entry for fast followers is significantly less resource intensive than this section would initially suggest [45]. Again, emphasising the enormous responsibility of national counterintelligence capabilities to secure the IP at every point in the supply chain to ensure entry barriers remain high and threat actors are barred from access. Thus, an escalation in cost.

However, the initial costings for a first mover can also prove unpredictable. Developing autonomous systems involves the procurement of sophisticated hardware and advanced software, along with the accumulation and management of vast amounts of data. These elements are essential to construct, operate, and regularly update the system. However, these components can be susceptible to considerable price fluctuations. The unpredictability of costs is largely determined by changes in market supply and demand, escalating geopolitical tensions, or dramatic shifts in economic policies. These factors can significantly alter the costs associated with the development, operation, and maintenance of military AI. Moreover, these uncertainties can hinder strategic planning and the ability to forecast future requirements accurately. They also complicate the allocation of defence budgets, which are typically subjected to rigorous scrutiny and oversight. For these reasons, the inherent cost volatility and unpredictability represent one of the most significant risks in integrating AI into military systems, especially because of the requirement for public scrutiny and accountability for projected spending vs. the value proposition. The development, implementation, and maintenance of AI-based systems necessitate a wide array of resources. This ranges from physical materials such as rare earth metals essential for manufacturing advanced electronics (chiefly Lithium [53]), semiconductors critical for data processing, and extensive data storage infrastructure, to human resources

with specialized skills in AI research, development, and deployment. A scarcity or interruption in the availability of any of these critical resources may lead to significant supply chain disruptions and costs [44]. Similarly, the known challenges faced by militaries to recruit and retain experts in relevant fields poses a significant barrier to the widespread adoption of AI in the military [44]. This deficit is further exacerbated by the fierce competition for talent from the private sector, where compensation often exceeds what the public sector can offer. Therefore, any strategic plan for the adoption of AI in the military must include a robust strategy for resource acquisition, management and retention to mitigate these risks.

An often overlooked yet significant factor in the discussion about the implementation of AI in military applications (such as autonomous aircraft) is the economic cost associated with regulatory compliance. Adherence to both international norms and domestic regulations governing the use of AI can impose substantial costs on defence departments and the associated industries. To start with, one of the significant expenses associated with regulatory compliance is related to data protection and privacy. The use of AI technologies often involves the processing of vast amounts of data, some of which may be personal or sensitive. Complying with data protection regulations can necessitate significant investments in secure data storage and processing infrastructure. For example, compliance with Europe's General Data Protection Regulation requirements was expected to cost large business an average of 1.3 million euros [54]. It also involves the continuous updating of security protocols and measures to prevent unauthorized access or data breaches. Implementing robust data management policies and procedures that are compliant with privacy laws, which vary from nation to nation, is a complex and costly task, but it is essential given the sensitive nature of military operations and the potential for misuse of personal data. In addition, certification processes can be costly and time-consuming, but they are often a necessary step in demonstrating that a system is safe, reliable, and compliant with regulations. Furthermore, regulations related to export controls can impose additional costs on the development and deployment of military AI systems. Again, these vary from country to country requiring in some cases a specialised team of experts on export controls to be organic to a company to assist in navigating multinational export contracts. Certain AI technologies may be subject to strict export controls, which can restrict the countries to which these technologies can be exported or shared. Navigating these regulations can require significant legal expertise and administrative resources. Breaches of these regulations can result in substantial penalties, including fines, sanctions, or even

prohibitions on the use of certain technologies. Beyond these direct costs, the changing nature of the regulatory landscape presents an ongoing challenge. As the implications and applications of AI continue to evolve, so too must the regulations govern its use. Staying abreast of these changes requires continuous monitoring and adaptation, further adding to the overall costs of regulatory compliance. Defence departments and AI developers must be prepared to adjust their policies, procedures, and systems in response to regulatory changes. This requires a level of agility and flexibility that can be costly to maintain but is crucial for ensuring long-term regulatory compliance. Overall, therefore, the cost component of regulatory compliance in the context of AI's integration into military systems can be significant. While the associated costs can be substantial, the implications of non-compliance, including potential fines, sanctions, and reputational damage, underscore the importance of investing in robust compliance mechanisms. The ability to navigate the complex and evolving regulatory landscape is not only a legal and ethical obligation but also a strategic necessity in leveraging the transformative potential of AI in the military domain responsibly and effectively.

Finally, it worth considering the risks introduced into critical supply chains through international venture capital flows and multinational business relationships. The multinational and dual-use of AI-enabled systems means that the ecosystem of commercial and research actors in the development of a given system are far broader than with more conventional modern military platforms [13]. This is particularly important in the case of autonomous systems and other military applications of AI because a failure point can be introduced (whether by accident or with malicious intent) at any stage of the process, for example in the collection, collation, and application of training data. As demonstrated by the finding of a Chinese-made alloy in the F-35 supply chain [39], the multinational web of companies involved in complex military industrial bases make it incredibly difficult for regulators to prevent supply chain intrusion. In this example it was simply an alloy, the security risk came from the potential for that firm to either input faulty parts or refuse supply. Contrastingly, the unknown participation of a compromised firm in the data training or base coding compilation for an AI technology could fundamentally undermine that system's reliability and effectiveness without necessarily leaving an identifiable trail. Focusing of excluding Chinese state-linked firms from sensitive supply chains (such as we have seen with Huawei [55]) risks overlooking another major potential source of advantage loss, either through acquisition, data leakage, or integration into adversaries' innovation networks leveraging access gained through venture capital investments and corporate acquisitions [46].

As noted by Sayler (2020), there has been a significant "wave of investment" by US venture capitalists in AI that reached approximately $18.5 billion in 2019 [47]. Of note is that by 2015 Chinese venture capital investment was involved in 16% of all contracting in Silicon Valley firms [48], and by 2018 it had reached approximately 69% of the global total venture capital spending [49]. Bolstered by state-backed venture capital funds, the latter's investment in promising AI startups in places like Silicon Valley present not just IP challenges in the short term, they also lay the ground for longer-term sustainment security concerns.

4. Conclusion

In conclusion, the spike in public and policy maker interest in AI in mid-2023 represents an inflection point, an opportunity to adopt a systems approach to understanding the processes by which such innovations are translated into reality. As civilian actors consider the implications of democratised large learning models, militaries continue to pursue increasingly AI-enabled autonomous weapon systems. Both inventions represent potential demonstration points for disruptive, and potentially destructive uses of AI, and in both cases one must devote significant technological consideration and policy resources to understanding, mapping and addressing the often overlooked risks associated with developing and producing the underlying technology. The supply chains for such advanced systems are complex, multi-nodal, and cross-jurisdictional. Securing each stage from intrusion without artificially slowing innovation is a challenge particularly for democratic governments, which have more limited options for directing commercial actors. Such policy makers should be encouraged by the academic community to have meaningful discussions toward effective resilience building measures across the supply chain. Such resilience must be build early and reinforced in a multinational manner to ensure that future AI-enabled autonomous systems and other forms of military AI are developed, produced and deployed in a responsible and effective manner. Future avenues for research in this space would include evaluating mechanisms for collaborative development of AI safeguards for military systems, developing common concepts of operations for future deployment of autonomous systems in strategic logistics, and the potential for European Union members to develop integrated AI-enabled supply chains.

References

[1] A. Wyatt, *The Disruptive Impact of Lethal Autonomous Weapons Systems Diffusion: Modern Melians and the Dawn of Robotic Warriors*. Oxon and New York: Routledge, 2021.

[2] E. B. Kania. (2019). Chinese military innovation in artificial intelligence. Testimony to the US-China Economic and Security Review Commission. [Online]. Available: https://www.cnas.org/publications/congressional-testimony/chinese-military-innovation-in-artificial-intelligence. [Accessed: Jan. 22, 2023].

[3] F. Sauer, "Stopping 'killer robots': Why now is the time to ban autonomous weapons systems," *Arms Control Today*, vol. 46, no. 8, pp. 8–13, 2016.

[4] Office of the Under Secretary of Defense for Policy, Directive 3000.09, United States Department of Defense, 2012.

[5] Development, Concepts and Doctrine Centre, Joint Concept Note 1/18: Human-Machine Teaming, United Kingdom Ministry of Defence, 2018.

[6] Robotic and Autonomous Systems Implementation & Coordination Office, Robotic & Autonomous Systems Strategy v2.0, Canberra: Australian Army, 2022.

[7] M. C. Horowitz, "Why Words Matter: The Real World Consequences of Defining Autonomous Weapons Systmes," *Temple International and Comparative Law Journal*, vol. 30, pp. 85–98, 2016.

[8] P. Scharre, *Four Battlegrounds: Power in the Age of Artificial Intelligence*. New York: ww Norton, 2023.

[9] H. M. Roff, "The strategic robot problem: Lethal autonomous weapons in war," *Journal of Military Ethics*, vol. 13, no. 3, pp. 211-227, 2014, doi: 10.1080/15027570.2014.975010.

[10] I. Bode, H. Huelss, and A. Nadibaidze, "Written Evidence AIW 0015," presented at the UK House of Lords AI in Weapon Systems Select Committee, 4 May 2023. [Online]. Available: https://committees.parliament.uk/writtenevidence/120184/pdf/. [Accessed: Jun. 6, 2023].

[11] L. Righetti, N. Sharkey, R. Arkin, D. Ansell, M. Sassoli, et al., "Autonomous weapon systems: technical, military, legal and humanitarian aspects," Proceedings of the International Committee of the Red Cross. Geneva, Switzerland, pp. 26–28, 2014.

[12] A. Wyatt, "Charting great power progress toward a lethal autonomous weapon system demonstration point," *Defence Studies*, vol. 20, no. 1, pp. 1–20, 2020, doi: 10.1080/14702436.2019.1698956.

[13] A. Ghadge, Maximilian Weiß, Nigel D. Caldwell, and R. Wilding, "Managing cyber risk in supply chains: A review and research agenda," *Supply Chain Management: An International Journal*, vol. 25, no. 2, pp. 223–240, 2020, doi: 10.1108/SCM-10-2018-0357.

[14] S. Abaimov and M. Martellini, "Artificial intelligence in autonomous weapon systems," 21st Century Prometheus: Managing CBRN Safety and Security Affected by Cutting-Edge Technologies, pp. 141–177, 2020.

[15] M. C. Horowitz, *The diffusion of military power (The Diffusion of Military Power)*. Princeton, NJ: Princeton University Press, 2010.

[16] A. Wyatt and J. Galliott, "The revolution of autonomous systems and its implications for the arms trade," in *Research Handbook on the Arms Trade*, A.T.H. Tan, Ed. Cheltenham and Northampton, MA: Edward Elgar Publishing, 2020, pp. 389–405.

[17] A. B. Silverstein, "Revolutions in military affairs: A theory on first-mover advantage," B.A. thesis, University of Pennsylvania, Philadelphia, 2013.

[18] J. Kwik, "Mitigating the Risk of Autonomous-Weapon Misuse by Insurgent Groups," *Laws*, vol. 12, no. 1, 2023, doi: 10.3390/laws12010005.

[19] K. Chávez and O. Swed, "The proliferation of drones to violent nonstate actors," *Defence Studies*, vol. 21, no. 1, pp. 1–24, 2021, doi: 10.1080/14702436.2020.1848426.

[20] M. I. B. Amirruddin, "How Threat Assessments Can Become Self-Fulfilling Prophecies," Pointer, vol. May, 2023.

[21] R. Gilpin, "The theory of hegemonic war," The Journal of Interdisciplinary History, vol. 18, no. 4, pp. 591–613, 1988, doi: 10.2307/204816.

[22] S. Shead, "UN talks to ban 'slaughterbots' collapsed — here's why that matters," in CNBC, ed, 2021.

[23] B. Zhang, M. Anderljung, L. Kahn, N. Dreksler, M. C. Horowitz, and A. Dafoe, "Ethics and governance of artificial intelligence: Evidence from a survey of machine learning researchers," *Journal of Artificial Intelligence Research*, vol. 71, pp. 591-666-591-666, 2021, doi: 10.1613/jair.1.12895.

[24] A. Wyatt and J. Galliott, "An Empirical Examination of the Impact of Cross-Cultural Perspectives on Value Sensitive Design for Autonomous Systems," *Information*, vol. 12, no. 12, p. 527, 2021, doi: 10.3390/info12120527.

[25] J. Galliott and A. Wyatt, "A consideration of how emerging military leaders perceive themes in the autonomous weapon system discourse," *Defence Studies*, vol. 22, no. 2, pp. 253–276, 2022, doi: 10.1080/14702436.2021.2012653.

[26] [A. Blanchard and M. Taddeo, "Autonomous weapon systems and jus Ad Bellum," AI & SOCIETY, pp. 1–7, 2022, doi: 10.1007/s00146-022-01425-y.

[27] E. Riesen, "The Moral Case for the Development and Use of Autonomous Weapon Systems," *Journal of Military Ethics*, vol. 21, no. 2, pp. 132–150, 2022, doi: 10.1080/15027570.2022.2124022.

[28] R. Waters, "Falling costs of AI may leave its power in hands of a small group," Financial Times, 10 March 2023. [Online]. Available: https://www.ft.com/content/4fef2245-5559-4661-950d-6eb803fea329. Accessed: Jun. 6, 2023].

[29] D. Nikolaiev, *Behind the Millions: Estimating the Scale of Large Language Models,* 2023. [Online]. Available: https://towardsdatascience.com/behind-the-millions-estimating-the-scale-of-large-language-models-97bd7287fb6b. [Accessed: Jun. 6, 2023].

[30] M. DeGuerin, "'Thirsty' AI: Training ChatGPT Required Enough Water to Fill a Nuclear Reactor's Cooling Tower, Study Finds," in Gizmodo, 2023. [Online]. Available: https://gizmodo.com/chatgpt-ai-water-185000-gallons-training-nuclear-1850324249. [Access: Accessed: Jun. 6, 2023].

[31] U. Gal, "ChatGPT is a data privacy nightmare. If you've ever posted online, you ought to be concerned," in University of Sydney News, 2023. [Online]. Available: https://www.sydney.edu.au/news-opinion/news/2023/02/08/chatgpt-is-a-data-privacy-nightmare.html. [Accessed: Jun. 6, 2023].

[32] B. Martin, L.H. Baldwin, P. Deluca, S. Henriquez, N. Hvizdaet et al., *Supply Chain Interdependence and Geopolitical Vulnerability: The Case of Taiwan and High-End Semiconductors.* Santa Monica: Rand Corp.

[33] K. Devitt, M. Gan, J. Scholz, R. Bolia, "A Method for Ethical AI in Defence," *Defence Science and Technology Group*, Contract No.: DSTG-TR-3786, 2021.

[34] T. Phillips-Levine. (2023). *War on the Rocks* [Online]. Available: https://warontherocks.com/2023/05/the-art-of-supply-chain-interdiction-to-win-without-fighting/. [Accessed: Jun. 6, 2023].

[35] M. Brundage, S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, et al. "The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation," 2018. doi: 10.48550/ARXIV.1802.07228.

[36] C. Strike, "Global Threat Report," *CrowdStrike*, 2023.

[37] V. Boulanin, *Mapping the development of autonomy in weapon systems: A primer on autonomy*. Stockholm: Stockholm International Peace Research Institute, 2016.

[38] A. Mehta, *Experiment over: Pentagon's tech hub gets a vote of confidence* [Online]. Available: https://www.defensenews.com/pentagon/2018/08/09/experiment-over-pentagons-tech-hub-gets-a-vote-of-confidence/. [Accessed: Jun. 6, 2023].

[39] L. Hudson, *Pentagon to resume F-35 deliveries after Chinese materials discovered*, Politico, 2022 [Online]. Available: https://www.politico.com/news/2022/10/07/pentagon-f-35-deliveries-chinese-materials-00060962. [Accessed: Jun. 6, 2023].

[40] R. Neuhard, *Foreign Policy Research Institute*, 2022. [Online]. Available: https://www.fpri.org/article/2022/10/the-new-us-national-security-strategy-four-takeaways-for-asia-policy/. [Accessed: Jun. 6, 2023].

[41] A. Holland Michel, "The black box, unlocked: predictability and understandability in military AI," United Nations Institute for Disarmament Research, 2020. doi: 1037559/SecTec/20/AI1.

[42] E. H. Christie, A. Ertan, L. Adomaitis, M. Klaus, "Regulating lethal autonomous weapon systems: exploring the challenges of explainability and traceability," AI Ethics, 2023. doi: 10.1007/s43681-023-00261-0.

[43] J. Haner, D. Garcia "The artificial intelligence arms race: Trends and world leaders in autonomous weapons development", *Global Policy*, vol. 10, no. 3, pp. 331–337, 2019, doi: 10.1111/1758-5899.12713.

[44] E. Schmidt, R. Work, S. Catz, E. Horovitz, S. Chien, A. Jassy, et al. "Final Report: National Security Commission on Artificial Intelligence (AI)," National Security Commission on Artificial Intelligence, Contract No.: AD1124333, 2021.

[45] A. Wyatt, J. Galliott, "Toward a Trusted Autonomous systems Offset Strategy: Examining the Options for Australia as a Middle Power," Australian Army Research Centre, Contract No.: 2, 2021.

[46] S. Korreck, "Exploring the Promises and Perils of Chinese Investments in Tech Startups: The Case of Germany," Observer Research Foundation, 2021.

[47] K. M. Sayler, "Artificial Intelligence and National Security," Congressional Research Service, Contract No.: R45178, 2020.

[48] M. Brown, P. Singh, "China's Technology Transfer Strategy: How Chinese Investments in Emerging Technology Enable A Strategic Competitor to Access the Crown Jewels of U.S. Innovation," Defense Innovation Unit – Experimental, 2018.

[49] E. H. Christie, C. Buts and C. Du Bois, "America, China, and the struggle for AI supremacy," 24th Annual International Conference on Economics and Security, Volos, Greece, July 8–9, 2021.

[50] M. C. Horowitz, "Artificial intelligence, international competition, and the balance of power," *Texas National Security Review*, vol. 22, 2018, doi: 10.15781/T2639KP49.

[51] M. Lamberth, P. Scharre, "Arms Control for Artificial Intelligence," *Texas National Security Review*, vol. 6, no. 2, pp. 95–110, 2023, doi: 10.26153/tsw/46142.

[52] S. Writer, "Fact Check-Simulation of AI drone killing its human operator was hypothetical, Air Force says," in *Reuters*, 2023. [Online]. Available: https://www.reuters.com/article/factcheck-ai-drone-kills-idusL1N38023R/ [Accessed: Dec. 4, 2023].

[53] E. Jones, B. Easterday, "Artificial Intelligence's Environmental Costs and Promise," in *Council on Foreign Relations*, 2022. [Online]. Available: https://www.cfr.org/blog/artificial-intelligences-environmental-costs-and-promise [Accessed: Dec. 4, 2023].

[54] L. Irwin, "How Much Does GDPR Compliance Cost in 2023?," in *IT Governance*, 2023. [Online]. Available: https://www.itgovernance.eu/blog/en/how-much-does-gdpr-compliance-cost-in-2020 [Accessed: Dec. 4, 2023].

[55] J.-Y. Lee, E. Han, and K. Zhu, "Decoupling from China: how US Asian allies responded to the Huawei ban," *Australian Journal of International Affairs*, vol. 76, no. 5, pp. 486-506, 2022, doi: 10.1080/10357718.2021.2016611.

[56] G. Baryannis, S. Validi, S. Dani, G. Antoniou, "Supply chain risk management and artificial intelligence: state of the art and future research directions," *International Journal of Production Research*, vol. 57, no. 7, pp. 2179–2202, 2019, doi: 10.1080/00207543.2018.1530476.

[57] R. Fedasiuk, J. Melot, B. Murphy, Harnessed lightning: *How the Chinese military is adopting artificial intelligence*. Washington DC: Center for Security and Emerging Technology, 2021.

[58] F. E. Morgan, M. Boudreaux, A. J. Lohn, M. Ashby, C. Curriden, et al., *Military applications of artificial intelligence*. Santa Monica: RAND Corporation, 2020.