“These are Not the Droids You’re Looking For”:

The Reality of AI, US National Security, and Global Power Dynamics

Ella Grady

PSCI 299 - Cyber & AI: National Security Impact

May 6, 2024

Introduction

In the past few years, Artificial Intelligence (AI) has made a large splash, as awareness of the technology has spread to the greater public, seemingly emerging from nowhere, fully formed, raising concerns about how to monitor and regulate these AI systems. In reality, AI has been an area of interest, particularly for the United States government, since the 1950s, driven initially by the Cold War need for applied technology. The recent surge in concerns over AI has raised questions about how it can be used to boost national security and change the nature of security threats. Competition over who will become the leading power in the new world of AI has begun, and with demonstrated action from China and Russian President Vladimir Putin proclaiming that the leader of AI will become the ruler of the world, it has increased pressure on the US to maintain its position as the global tech leader. President Biden has made AI a focus of his administration, pushing for greater efforts to pursue improved technology. With all these factors, the proposed research question guiding this paper and my research was: how do advancements in artificial intelligence and related technologies pose threats to US national security and what can be done to mitigate and combat those threats?

Common fears of AI focus on singularity – the theoretical idea that there will be a point at which AI becomes more intelligent and cuts humans out of the loop. Currently, singularity is a long way off, if even possible (Boden 2014, 147-148). It is a level that only exists in science fiction novels and should not be considered a legitimate worry about AI’s impacts currently. That is not to say there are not many factors of AI to be wary of, particularly in the context of national security. AI has been increasingly used and will continue to be used in defensive and offensive strategies, and at this point, there have been limited efforts to create global agreements on the extent to which this technology can be used. One example is the United Nations General Assembly's joint statement on regulating autonomous weapons, which has yet to reach regulatory implementation (Automated Decision Research 2023a, 4). While AI will have implications on defense weapons that will change the landscape of war and security, advancements in artificial intelligence and their implementation in national security strategies pose greater threats with the effects they can have on global power dynamics and international relations. Mitigating these risks will take global cooperation on agreements and treaties regulating the use of AI, public campaigns, and a widespread understanding of the ethical and moral considerations when using AI. This paper will explore current AI-related threats to US national security, both through direct technology deployments and through global power dynamics, as well as potential mitigation and combat strategies to counteract these threats. To demonstrate the current situation, a case study of lethal autonomous weapons systems will be presented to exemplify the discussions on the effectiveness, challenges, and limitations of different strategies for mitigating AI threats.

Literature Review

Scholarship on this topic tends to be divided along several lines among the subtopics of threats and mitigation strategies. Works on national security threats posed by AI are typically split between focusing on direct versus indirect threats, while the work on strategies divides the proposed strategies between defensive and deterrence. Typically through a realist lens of international relations, much of the literature focuses on the awareness states have of the international balance of power, the competition to gain the advantage at the expense of others, and the interest in the balance of power required by the structure of the international system to ensure survival in the world of evolving AI technologies (Ndzendze and Marwala 2023, 57).

The commonly identified direct threats in the literature are as follows: improved deployments of adversarial warfare technologies (including autonomous weapons), cybersecurity attacks, and information warfare capabilities. These works generally find that while these technologies existed previously, AI will improve the capabilities and impact of these technologies (Allen and Chan 2017, 2, 21; Sayler 2020, 11-12). In contrast, the literature on indirect threats typically focuses on global power dynamics, encompassing the idea of an AI race between global powers and the implications of competition causing the security dilemma, as well as the potential for limited knowledge and misunderstandings of the state of other nation's technology (Horowitz 2018, 42, 55; Sacks 2023, 17). One scholar, Michael Horowitz, for example, believes this impact on power dynamics will arise because of AI's impact on the economy as military superiority over the long term can only occur if there is an underlying economic basis, arguing that the economic impact of corporate development and competition in AI globally will be a significant determinant in this race (2018, 42). Furthermore, amongst those discussing the security dilemma, the general consensus is that the security dilemma is heightened by the uncertainty of the reliability of these technologies and the competitive nature causing a cycle of racing to remain on top (Sacks 2023, 18; Scharre 2021, 124).

Writings about the strategies for mitigating national security threats posed by AI tend to either focus on preventative or potential reactionary strategies. The discourse on preventative strategies focuses on typical security-building strategies such as deterrence, signaling, confidence-building measures, and regulatory frameworks and policies, for example, the threat of second-strike capabilities or the UNESCO Recommendation on Ethics of AI from 2021. The reasoning behind many of these strategies centers on the idea of signaling a state's awareness of the need to exercise caution and the importance of encouraging collaborative efforts to come to agreements (Sacks 2023, 21; Horowitz and Scharre 2021, 4; Talberg et al. 2023, 6). Works on strategies that are more reactionary include implementing defensive and response technologies to prevent or mediate attacks, for which recommendations included threat identification and analysis, tools for finding cybersecurity vulnerabilities and patching remedies, predictive maintenance of defense systems in operational logistics, and command decision support through data analysis (Mori 2018, 27-30). The reasoning behind these recommendations connects back to the security dilemma – one state implementing AI technologies will cause others to implement, and the best way to protect against these AI systems will be to use AI itself.

Research Methodology

To understand the AI threats to national security and potential mitigation strategies, a qualitative case study on lethal autonomous weapons systems (LAWS) is presented. LAWS were selected, despite the fact no state has implemented them yet (at least to public knowledge), because there has been interest globally in pursuing them, and for many states, they raise ethical concerns that could impact security goals (Sayler 2020, 7-8; Daniels 2022, 16). This study focuses on summarizing and analyzing information from primary and secondary sources, as collecting empirical data on military weapons systems was not possible for this research due to the restricted accessibility of information about current developments in the defense industry. To do so, existing research from several think tanks, government reports, and non-governmental agency statements was used to understand the general consensus and situation surrounding the implementation of LAWS. Particularly useful were statements from the United Nations General Assembly meetings and context from the United Nations Office of Disarmament Affairs.

Background and Context to Current AI Technology

Artificial Intelligence (AI) is a term often thrown around, but generally, clarity is lacking on the type or focus of a given AI technology. It is a broad term that encompasses language models, generative systems, robotics, deep learning technologies, and more. As it stands, there is no widely accepted definition of AI, though it can generally be defined as the ability of a computer system to complete tasks that typically require human intelligence (Cummings 2017, 2). To understand the risks of AI, it is first crucial to understand the types of AI and how they differ. At the most basic there are two classifications of AI systems: Narrow AI and General AI (Allen and Chan 2017, 8). Narrow AI are systems that are designed for specific tasks, within a predefined range, using pre-established rules and algorithms; all current instances of AI are narrow. General AI, a theoretical concept at this time, are systems that can understand, learn, and apply its intelligence to solve any problem, like humans. These systems would be able to comprehend the context of their tasks, learn from experience, and make judgments in unfamiliar situations (Sayler 2020, 2). Currently, the most popular and well-known AI tools are predictive, generative systems, such as OpenAI's ChatGPT, Google's Gemini, and Outlook's text prediction. These systems generate content, ideas, or data based on user input through algorithms and data set analysis training.

Other important terms to understand in considering AI and national security are machine learning and autonomous systems. Machine learning involves using algorithms to replicate cognitive thinking processes with procedures derived through the analysis of large training data sets (Scharre 2023, 2). Machine learning in national security applications can look like data analysis tools, image recognition in drones, and cybersecurity technique boosting (Sacks 2023, 20; Strayer 2023, 3). Autonomous systems, such as robots, weapons, or drones in the security realm, are not the same thing as AI, but AI is becoming foundational in enabling these systems. These systems can function without human intervention or oversight, though humans are involved in their training and enabling.

Broadly, AI is being introduced across all industries and sectors. It has become a household technology with products like ChatGPT, DALL-E, and Gemini spurring conversations about the ethics and implications of using AI technology. AI has been employed in industries like healthcare, finance, and e-commerce to boost productivity and efficiency, through services such as imaged disease detection, fraud detection, and trend prediction, respectively (Q.ai 2023). In the national security and military realm, specifically, AI is being employed directly for intelligence analysis, threat identification, cybersecurity, and logistical understanding. It is also being integrated into systems like unmanned vehicles, autonomous defense systems, decision-making processes, and drones (Daniels 2022, 16-17). Not only can AI be directly implemented or integrated into national security defense tools, but it can also aid in strengthening other technology, e.g., system maintenance tools and cyber defense mechanisms.

There has been significant discussion surrounding the introduction of AI as a new industrial revolution, bringing about new societal processes, and transforming society with intelligent machines, similar to the changes of mechanization in previous industrial revolutions (Scharre 2023, 4). With these developments and the introduction of AI to defense, AI systems have begun a revolution in military affairs, similar to the changes brought to warfare by the introduction of firearms (Horowitz 2018, 43). Beyond the physical changes to war landscapes through technological developments, AI also poses threats to national security due to its potential effects on global power dynamics and international relations.

AI's Threats to National Security

With the increased interest in and rapid development of artificial intelligence, many sectors have been transformed, including national security. With the idea of AI as a new industrial revolution, comes new revolutions in military affairs. This section dives into the various, multifaceted threats AI poses to national security, ranging from direct technological vulnerabilities to subtler nuances of global power dynamics. By examining areas like cybersecurity, autonomous warfare, and the strategic competition of major powers, this analysis highlights the increased need for comprehensive strategies to mitigate these emerging risks. As

AI continues to evolve and transform, understanding these threats and the technology is imperative for maintaining national and global security.

Direct Threats

Cybersecurity

With the normalized dependence on electronics, telecommunications, and cyber control of infrastructure, the United States has grown more vulnerable to cyberattacks. Cyberattacks are deliberate actions intended to alter, disrupt, deceive, or destroy computer systems or networks and the information or programs stored on or transmitted between these systems. In 2010, the Department of Homeland Security identified cyberattacks as one of the most severe threats to US security, labeling cyberspace a domain equivalent to land, sea, or air (Caplan 2013, 94). Cyberattacks on US security measures are done for many reasons, including economic espionage, counterintelligence, retaliation, intimidation, coercion, and with the intent of harming or changing the global landscape or disrupting established ways of life (Carlin 2016, 404-407).

Cyberattacks were already cheap and relatively easily achievable for adversaries. The introduction of AI enhances the capabilities of cyber attackers by automating the attack generation and improving the speed and sophistication of these attacks, increasing the significance of this as a threat to national security infrastructures (Payne 2021, 107-108). Beyond enhanced cyberattacks, also come concerns over vulnerabilities in AI systems that can be exploited through cyberattacks. The AI systems themselves can be susceptible to various forms of cyberattacks, such as data poisoning, model stealing, and adversarial attacks. Machine learning systems can be incorrectly trained if the data is biased or has been tainted by an adversary, making AI systems a new class of cyber vulnerabilities for national security and a new opportunity for exploiting other nation’s systems (Scharre 2023, 238).

Warfare Autonomy

Not only can AI be perceived as an industrial revolution, but it also can be viewed as a revolution of military affairs, just like the historical advancements that transformed warfare, such as firearms. AI is setting new patterns and standards for military strategy and capabilities. Many fears about AI in warfare focus on fully autonomous weapons systems and decision-making without human oversight. Concerns about the use of autonomous weapons systems focus on the potential for these technologies, powered by AI, to increase human suffering, make war more likely, and negatively impact national security overall (Horowitz et al. 2020, 529). Lethal autonomous weapons systems – machines capable of searching, selecting, and engaging targets without human intervention – are one such example of AI systems dangerous to security and global stability (Scharre 2023, 286). Furthermore, a greater risk is the impact autonomous AI-powered systems could have on nuclear stability. This could come through undermining a nation's security strategies of nuclear deterrence, increasing the risk of a first strike, creating more reliance on nuclear weapons by improving conventional military forces, or direct integration of AI into nuclear operations (Scharre 2023, 288).

It is also important to understand the impact autonomous weapons systems can have on the concepts of deterrence and credibility. In a simulated war game conducted by the RAND Corporation, it was seen that deploying autonomous weapons systems could affect extended deterrence and the ability to maintain credibility in reassuring allies of US commitment. On one hand, deploying autonomous systems could enhance the credibility of US extended deterrence because the risk to personnel is much lower and more quickly actionable, suggesting a higher willingness to act. On the other hand, allies could interpret an increased reliance on autonomous systems as a detriment to US credibility because of a perceived unwillingness to put American lives at risk in severe crisis (Huh Wong et al. 2020, 59-60). Furthermore, widespread implementation of AI and autonomous systems could lead to higher chances of escalation and crisis instability, as dynamics are formed that are conducive to rapid and unintended crisis and conflict escalation due to the quick speed of decision-making if done at the machine level, rather than by humans (Huh Wong et al. 2020, 60). Deploying autonomous systems in crises could also increase the risk of accidents and miscalculations (Horowitz and Scharre 2021, 18), as the quick decision-making turnaround time, with limited human oversight, does not allow time for further developments and considerations.

Information Warfare

Beyond weapon systems, AI can impact security through information warfare campaigns. Particularly when combined with cyberattacks or social media network flooding, AI-generated media can threaten the stability and security of a government. In April 2013, hackers took control of the official Associated Press Twitter account and posted news of explosions in the White House injuring Barack Obama, causing the US stock market to lose $136 million before the hack was revealed. Adding AI-enabled media generation raises the potential for more costly and devastating hacks. In this scenario, not only would hackers have control of official websites or social media accounts to spread false news, but also convincing fake video, audio, or images, that could be quickly spread to influence the public through a network of bot accounts (Allen and Chan 2017, 33). Depending on the news, such a campaign could cause rioting, stock market crashes, or impact the state's credibility with its allies, its security, and stability.

Indirect Threats of Global Power Dynamics

Not only can AI have direct technological impacts on threats to national security, but it also has the potential to impact global power dynamics, posing threats to security as dynamics shift. Many scholars of the topic have suggested that the competition over AI will occur across the globe as most states race to keep up with development, but the key players vying for the position of global leader, as Putin commented, will be the US, China, and Russia (Huh Wong 2020, 5). The competition for AI superiority between these countries heightens tensions and escalates a security dilemma with the perception of each other's technological advances as direct threats. Like the escalation potential of autonomous weapons, the increasing rush for AI technologies in national security could lead to a security dilemma over the increasing pursuit of countermeasures, creating a cycle of uncertainty and less security (Huh Wong 2020, 61). This is also important to understand as governments encourage industry investments in AI and improve AI tools for security. For example, leading AI companies such as OpenAI, Microsoft, Google, and NVIDIA are all US-based companies leading in the field, with interest and investments from the US government to improve AI technology for use by the state (Scharre 2023, 32). To maintain a position as a leader in AI, the US needs a policy framework that is pro-innovation, prioritizing innovation and investment in private industry (Strayer 2023, 9). Industry is where the top researchers are headed, as private corporations have fewer regulations and looser frameworks for development than the government. Many companies have expressed hesitation in partnering with the government because of the complexity of the defense acquisition process or ethical concerns over government use of AI for surveillance or weapon systems (Sayler 2020, 18-20).

On the other side, China has pursued AI joint government-industry development. In their 2017 "Next Generation AI Development Plan," they aimed to spend approximately $21.7 billion investing in the AI industry by 2020, to reach world-leading levels by 2030 in AI. Chinese development of AI for use in their security operations is largely influenced by their perceptions of US plans for defense innovation and concerns about a widening capability gap with the US military. Furthermore, there are fewer boundaries between private innovation and the Chinese government, as compared to the US, allowing the state to have more direct involvement in guiding AI development and accessing industry tech (Sayler 2020, 21-22). In contrast to both the US and China, Russia lags in its AI innovation, both in industry and in government. It is, however, an outlined plan and goal of the state to pursue technology to close the gap, and their relationship with China may give them a leg up in in the competition (Sayler 2020, 25-26).

Regardless of the relationship between industry and the government, innovation and a thriving AI industry can lead to a perceived security dilemma for adversaries. As long as the US has leading AI companies and researchers, the country will be seen as a competitor and someone to surpass in innovation by adversaries like China and Russia. Creating a cyclical dilemma, this ongoing competition will only drive the US government to further push its industry to develop strong technologies to maintain the lead, viewing, to quote Senator Ted Cruz, that "ceding leadership...to China, Russia, and other[s]...will...place the United States at a technological disadvantage, [and] could have grave implications for national security" (Sayler 2020, 20), positioning AI competition as an important consideration for protecting national security.

When considering shifting global power dynamics, it is also important to broadly consider how deterrence could be altered. Like the discussion of the security dilemma, deterrence can be impacted by the level of understanding of the adversary and their AI capabilities. Underestimating or misinterpreting the adversary could negatively impact deterrence strategies, but having an up-to-date and deep understanding could allow strategies to be shaped to meet the current circumstances. Societal experience and understanding of AI are also significant to consider, as the level of public trust and faith in AI can influence the confidence government representatives may have, or decisions that can be made, thereby influencing strategies of deterrence. The level of sophistication of AI technologies and the methods of employment will also be critical for better understanding the capabilities and focus of the AI systems that will infer what strategies should target (Huh Wong 2020, 27). Furthermore, the implementation of AI systems and technologies can change the confidence in US deterrence strategies for allies, and the fear of the threat by adversaries, as discussed earlier in the paper. This could either have a positive impact, leading to greater trust in the defense commitment because there are fewer American lives at risk and less incentive to avoid engaging, or it could have a negative impact with greater doubt because there is less skin in the game.

Mitigation Strategies for Protecting National Security

In the discourse, the global AI push is frequently compared to that of the nuclear arms race or the space race, due to the competitive nature, economic impact, and innovation across the military and civil sectors (Tallberg et al. 2023, 9; Allen & Husain 2017). Though similarities exist, both Paul Scharre and Michael Horowitz argue that these comparisons are not quite accurate. To start, Scharre opposes the conflation of the AI competition to the nuclear arms race, believing that global AI development, though competitive and having potential risks to national security, does not meet the definition of an arms race, particularly because AI is not inherently a weapon (2021, 122). With Scharre's argument in mind, it may make more sense to compare AI development to the space race, however, Horowitz would disagree to an extent, at least. Horowitz's argument centers around the bilateral nature of the space race between the Americans and the Soviets, compared to the multilateral global nature of the AI race. Furthermore, Horowitz posits that the space race was run by two governments for national purposes, unlike the primary focus of dual-use economic gain pushing commercial development of AI over military usage (2018, 51). Though believing the space race to be an inaccurate comparison, Horowitz admits the analogy can be useful to understand "the stakes in ways that generate incentives for bureaucratic action at the government level, and raises corporate and public awareness" (2018, 55).

While these arguments are important to understand to prevent misinterpretations of global power dynamics in this new race of development, the comparisons can be useful for applying similar strategies and lessons and understanding the importance of innovation. The US remained a leader in both the nuclear arms race and the space race due to its devotion to promoting innovation and collaboration between the private and public sectors (Allen and Husain, 2017). Past strategies like arms control agreements, national standards, and international regulations, such as confidence-building measures or conventions could inform proactive and deterrent AI security strategies, in addition to backup reactionary tools or strategies for defense.

International Regulations and Policy Measures

Regulatory measures to mitigate the risks of global military AI competition are one way to reduce the security threats of AI by providing confidence and reassurance for more than one state. This can be done by either expanding existing international frameworks to include AI-enhanced military weapons and systems or by proposing new international agreements specifically designed to address the deployment and development of AI globally, negotiating internationally accepted rules and norms to leverage and increase the benefits of AI, while also limiting any negative potential consequences (Tallberg et al. 2023, 2).

One existing framework recommended for expansion to include AI considerations is the UN's Convention on Certain Conventional Weapons (CCW). The CCW, an international legal structure, was established to focus on restricting or banning weapons considered to cause unjustifiable suffering or to have indiscriminate effects (Meier 2016, 119). Currently, the CCW does not explicitly regulate AI military technology, such as autonomous weapons systems, but could be a forum for advancing such regulations. Recent meetings have explored the implications of such technologies, highlighting the adaptability of the CCW to include AI

(United Nations 2023). Modifications to the CCW, and similar frameworks, could include specific provisions on the development, testing, and deployment of AI systems for military applications, to ensure they comply with international humanitarian law.

Adapting existing frameworks could prove difficult due to limitations of the structure or previous applications, and as such there is also a need for new international agreements to address the deployment and development of these technologies directly. Examples of this can include regulations with more civilian focuses, as many of these AI developments, especially in the US, are starting in the private sector. Examples of these are UNESCO's recommendations on the ethics of AI and the European Union's AI legislation (Tallberg et al. 2023, 2). These agreements focus on providing ethical guidelines for the scope and reach of AI development, primarily in the commercial sphere, across international borders. Despite that, they are good examples of agreements that can be built out to also encompass military applications, ensuring transparency, accountability, and commonly agreed-upon standards for AI usage, particularly with concerns for applications affecting security and human rights.

Horowitz and Scharre discuss that while many recent proposals for common standards and agreements on AI are not enforceable or verifiable, they can be useful for promoting shared norms and as early building blocks for more enforceable regulations (2021, 15). Implementation of international regulations will only be as useful as their enforcement, and while signing on to agreements is typically voluntary and requires self-identification of possession of systems, AI-related treaties can be modeled off such existing weapons treaties that have proved effective. One such example is the Chemical Weapons Convention which bans the possession of chemical weapons. This treaty conducts inspection and monitoring of states' relevant activities and relevant industry actions to ensure compliance (Arms Control Association n.d.). Similar requirements could be enforced for AI technologies to ensure commitment to treaties, even if the agreements aim for management over outright bans.

National Regulations and Frameworks for Internal Oversight

In addition to international agreements, nation-level confidence building for allies and potential adversaries can be employed through state-enforced regulations for the development, deployment, and maintenance of AI. Such confidence-building measures are designed to increase transparency, notification, and monitoring of risks due to military competition between states and can be done either through information sharing or inspection and observation measures. These measures can establish guiding operational rules, and limits to military readiness and operations (Horowitz and Scharre 2021, 10). Doing such things can boost a state's credibility for deterrence – for example, to deter adversaries by signaling capabilities for defense – and prevent misunderstandings of capabilities that could lead to instances of a security dilemma.

Defensive Technology

If AI is being deployed for military applications, it stands to reason that AI can also be used to boost defensive technologies to protect national security. This could look like threat identification and analysis; discovery of cybersecurity vulnerabilities and patching remedies; predictive maintenance of defense systems in operational logistics; and command decision support through data analysis (Mori 2018, 27-30). As AI technologies continue to develop and improve, the best way to defend against and reduce the threats arising from these systems is through the technology itself. To do so and maintain its position as a leader in this global competition, the US will need to invest in its workforce for innovation. US AI development is largely decentralized and minimally funded by the federal government. Corporate development, while beneficial for the general public and commercial uses, means the US lacks a cohesive national vision or standards, in comparison to China's highly centralized military AI development through its joint military-civil strategy (Daniels 2022, 13-14). Investing more in commercial partnerships, attracting more professionals in AI, and encouraging development and research to stay within the US will help protect the security of the US by maintaining its leading position in global AI development.

Case Study: Lethal Autonomous Weapons Systems

While many military applications of AI systems highlight the various threats to national security, a significant example warranting a case study is Lethal Autonomous Weapons Systems (LAWS). LAWS represent a significant shift in military technology and have been described as "the third revolution in warfare, after gunpowder and nuclear arms" (Sauer 2022, 237). LAWS are typically defined as weapons systems capable of selecting, targeting, and engaging adversaries independently, with limited human input, though this definition is not concrete. As Frank Sauer argues, "lethality" and "autonomy" are decisive characteristics that do not encompass the full scope of the issue, as for him the military application of non-lethal, but damaging force is also of concern. Furthermore, Sauer argues that in philosophical terms, describing computer systems as autonomous grants more agency to machines than is appropriate (2022, 238). Like many topics in AI, however, these terms are generally accepted and widely used, particularly given a common tendency to leap to the worst-case scenario.

While no state is, to public knowledge at least, currently employing fully autonomous lethal systems, the possibility remains an option and grows in likelihood as technology advances and competition becomes more contentious (Daniels 2022, 16; Longpre, Storm, and Shah 2022, 47). The earlier discussions of the benefits of autonomous systems for deterrence and credibility apply to LAWS. LAWS offer many tactical military advantages, such as faster reaction times and less direct human risk without troops manning the weapons. Assuming good data and effective training, LAWS have the potential to be more precise, executing coordinated attacks and reducing potential collateral damage and logistical burdens (Daniels 2022, 16).

Despite the advantages LAWS could have if employed, it is also critical to understand the risks posed by these systems. As discussed earlier, fully autonomous systems have a significant risk for accidental escalations due to the fast reaction time, particularly in systems where humans are cut out of the loop. Furthermore, as LAWS are computer systems, there is always the potential for hacking, malfunctions, or bad training and data that can bias the system, causing unpredictable outcomes that could negatively affect the security of the state (Longpre, Storme, and Shah 2022, 49). It is especially important to note the concerns about the unpredictability of warfare outcomes under autonomous systems and decision-making. Without a human-in-the-loop policy, it is possible for a great deal of uncertainty, more so than in traditional systems, as the human considerations of emotions, recognition of signaling, and morality concerns are potentially removed, making a system more likely to strike (Sacks 2023 18, 20). This potential, while concerning on its own, also poses a threat to national security, as other states perceive a threat to themselves, causing further ramp-ups of security defenses, triggering the race for the best technologies, and furthering the security dilemma in a never-ending cycle.

The international community's response to LAWS has been mixed. Some advocate for a total ban, while others favor regulated use. The United Nations has held multiple sessions to discuss the implications of autonomous weapons, and there are groups like the Campaign to Stop Killer Robots, focusing on the global concern over these technologies (United Nations n.d.). The US military's current policy requires humans to remain in the loop for any lethal autonomous weapons, though active development projects seem to contradict this policy. Despite this policy, the US is one of the states resisting efforts for international regulations (Longpre, Storme, and

Shah 2022, 47). For instance, the United States does not support the negotiation of legally binding international guidance on autonomous weapons systems or standards for human control (Automated Decision Research 2023b), preferring to keep open the possibility of reaping the benefits of speed and protection provided by LAWS (Longpre Storme and Shaha 2022, 47). Potential regulations and mitigation policies include the ban of fully autonomous weapons systems or national standards to continue to maintain human involvement in the loop, and while currently contradictory to US policy, these policies would ultimately protect US security.

Due to the risks posed by autonomous weapons systems to deterrence and credibility, not supporting the proposed regulations for these systems may, in the long run, damage the security of the United States. While some possibility of pursuing autonomous systems is a good potential defense system for the state, the belief of needing to maintain fully autonomous systems could be prohibited by international regulations for all states, removing this threat for everyone. Once fully autonomous systems are banned, partial autonomous systems that keep humans in the loop would be sufficient for maintaining security and minimizing the risks found in using autonomous systems, such as the misinterpretation of signals and lack of buffer time to consider the context that typically comes with human decision making.

Conclusion

This research has explored the impact of artificial intelligence on national security, highlighting its dual-sided potential to enhance defense capabilities and introduce significant risks. Conducting a case study on Lethal Autonomous Weapons Systems (LAWS) demonstrated the evolutionary role of AI in warfare, with discussions on the benefit of independent operation and potential risks such as accidental escalations and ethical challenges in autonomy. Furthermore, AI's role in shifting global power dynamics underscores the strategic importance of developing technology in international relations. By understanding these complexities, the findings of this work stress the need for robust mitigation strategies such as comprehensive regulatory frameworks and enhanced international cooperation, to effectively harness AI's potential while minimizing its risks.

The implications of this work extend beyond the theoretical discussions of international relations; they emphasize the need for immediate and concerted action to address the challenges of AI in security applications, such as LAWS. If left unchecked, these technologies could lead to an increased risk of unintended escalations, potentially drawing multiple countries into conflicts sparked by autonomous actions and decisions. Moreover, the rapid pace of AI development threatens to surpass the existing regulatory frameworks, leaving gaps that could be exploited by adversarial nations or non-state actors, threatening the security of the United States. This evolving landscape necessitates a robust response to prevent AI from becoming a destabilizing force in global dynamics, highlighting the importance of developing comprehensive governance frameworks to keep up with technological innovation and reinforce global stability and security.

The findings of this work should resonate across many groups, emphasizing the need for comprehensive and collaborative action. As Russian President Vladimir Putin said, whoever leads in AI will lead the world, and it has been shown that states, like China, are moving to take this space. This topic should be of importance and interest to anyone involved in national security and global stability, including policymakers, military strategists, and international groups. Beyond direct actors, this topic should also be of concern to anyone using AI, developing the technology, and the general public, as informed citizens are key to fostering support for policies and everyone should understand the stakes that will affect them in this new age of AI.

This research process was often limited by the inherent nature of the topic and data sources, a notable example being the inability to conduct empirical data collection on LAWS as this information is often kept in secrecy due to the sensitive nature of defense technology. Additionally, the research was primarily focused on US strategies and technologies, which do not fully encapsulate the global landscape of AI development. A lot of the discussion, especially predictions about future developments, is built on theoretical foundations and expert analysis rather than empirical evidence, highlighting the need for more data-driven research. Future research should also focus on continually evolving these ideas as the capabilities of AI develop, changing regulatory needs and ethical frameworks.

AI has the potential to impact almost every aspect of society, such as healthcare, education, and the media. As we navigate these changing dynamics, we can see the impacts present in areas like national security. In considering these impacts, this research highlights the urgent need for coordinated action and increased awareness. The dynamic interplay between technological innovation and geopolitical stability presented in this study demonstrates that AI is not only a tool of the future but a transformative force reshaping the global landscape. This paper has shown that without thoughtful regulation and ethical oversight, the advancements in AI could lead to increased risks of conflict and instability. However, with the right measures in place, these same technologies have the potential to enhance security, reduce human casualties in conflict zones, and foster international cooperation. Therefore, policymakers, military strategists, and technology developers must take a unified stance to reduce the risks posed by AI. This includes establishing clear guidelines for the development and use of autonomous systems, promoting transparency in AI research and deployment, and ensuring that all technological advances are matched with equal progress in ethical standards.

The role of AI technologies in national defense strategies has yet to be determined and shaped; that responsibility lies with us now as we balance an interest in maintaining a leading position and concerns for national security. By fostering an environment of international collaboration, the potential of AI can be harnessed responsibly as a determinant of peace and cooperation rather than conflict. Ultimately, the impact of AI on national security is significant and multi-faceted. As AI and our understanding of its full range of capabilities and risks continue to evolve, it is important to remain proactive and vigilant. The strategies and policies we implement today will not only determine future developments in AI but also the dynamics of international security for years to come.

References

Allen, Greg, and Taniel Chan. 2017. "Artificial Intelligence and National Security." *Belfer Center for Science and International Affairs*. Belfer Center for Science and International Affairs. https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf.

Allen, John R., and Amir Husain. 2017. "The Next Space Race Is Artificial Intelligence." *Foreign Policy*, November 3, 2017. https://foreignpolicy.com/2017/11/03/the-next-space-race-is-artificial-intelligence-and-america-is-losing-to-china/.

Arms Control Association. n.d. "The Chemical Weapons Convention (CWC) at a Glance." Accessed May 3, 2024. https://www.armscontrol.org/factsheets/cwcglance.

Automated Decision Research. 2023. "Convergences in State Positions on Human Control." 2. *Automated Decision Research*. https://www.stopkillerrobots.org/wp-content/uploads/2023/11/ADR_Convergences-in-state-positions-on-human-control.pdf.

———. 2023b. "USA | Automated Decision Research." November 21, 2023. https://automatedresearch.org/news/state_position/usa/.

Boden, Margaret A. 2016. "The Singularity." EBook. In *AI: Its Nature and Future*, 147–69. Oxford University Press. https://ebookcentral.proquest.com/lib/clarku/reader.action?docID=4545415&ppg=158.

Caplan, Nathalie. 2013. "Cyber War: The Challenge to National Security." *Global Security Studies* 4 (1): 93–115. http://goddard40.clarku.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=poh&AN=86149077&site=eds-live.

Carlin, John P. 2016. "Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats." *Harvard National Security Journal* 7 (2): 391–436. https://heinonline.org/HOL/P?h=hein.journals/harvardnsj7&i=392.

Cummings, M.L. 2017. "Artificial Intelligence and the Future of Warfare." *Chatham House*. https://chathamhouse.org/sites/default/files/publications/research/2017-01-26-artificial-intelligence-future-warfare-cummings-final.pdf.

Daniels, Owen J. 2022. "The 'AI RMA': The Revolution Has Not Arrived (Yet)." *The Andrew W. Marshall Foundation*. The Andrew J. Marshall Foundation. https://www.andrewwmarshallfoundation.org/wp-content/uploads/2022/11/AIRMA_FINAL.pdf.

Horowitz, Michael C. 2018. "Artificial Intelligence, International Competition, and the Balance of Power." *Texas National Security Review* 1 (3): 37–57. https://repositories.lib.utexas.edu/server/api/core/bitstreams/74307125-fc5e-4706-86fc-1b035e4bbfbc/content.

Horowitz, Michael C., Lauren Kahn, and Casey Mahoney. 2020. "The Future of Military Applications of Artificial Intelligence: A Role for Confidence-Building Measures?" *Orbis* 64 (4): 528–43. https://linkinghub.elsevier.com/retrieve/pii/S0030438720300430.

Horowitz, Michael C., and Paul Scharre. 2021. "AI and International Stability: Risks and Confidence-Building Measures." *Center for a New American Security*. Center for a New American Security. https://s3.us-east-1.amazonaws.com/files.cnas.org/documents/AI-and-International-Stability-Risks-and-Confidence-Building-Measures.pdf.

Huh Wong, Yuna, John M. Yurchak, Robert W. Button, Aaron Frank, Burgess Laird, Osonde A. Osoba, Randall Steeb, Benjamin N. Harris, and Sebastian Joon Bae. 2020. "Deterrence in the Age of Thinking Machines." *RAND Corporation*. RAND Corporation. https://www.rand.org/content/dam/rand/pubs/research_reports/RR2700/RR2797/RAND_RR2797.pdf.

Longpre, Shayne, Marcus Storme, and Rishi Shah. 2022. "Lethal Autonomous Weapons Systems & Artificial Intelligence: Trends, Challenges, and Policies." Edited by Kevin McDermott. MIT Science Policy Review. August 29, 2022. https://sciencepolicyreview.org/2022/07/mitspr-191618003019/.

Meier, Michael W. 2016. "Lethal Autonomous Weapons Systems (Laws): Conducting a Comprehensive Weapons Review." *Temple International and Comparative Law Journal* 30 (1): 119–32. https://heinonline.org/HOL/P?h=hein.journals/tclj30&i=127.

Mori, Satoru. 2018. "US Defense Innovation and Artificial Intelligence." *Asia-Pacific Review* 25 (2): 16–44. http://goddard40.clarku.edu/login?url=https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=133595632&site=ehost-live.

Ndzendze, Bhaso, and Tshilidzi Marwala. 2023. *Artificial Intelligence and International Relations Theories*. https://doi.org/10.1007/978-981-19-4877-0.

Payne, Kenneth. 2021. *I, Warbot: The Dawn of Artificially Intelligent Conflict*. Oxford University Press.

Q.ai. 2023. "Applications of Artificial Intelligence Across Various Industries." *Forbes*, January 6, 2023. https://www.forbes.com/sites/qai/2023/01/06/applications-of-artificial-intelligence/.

Sacks, Steven D. 2023. "A Framework for Lethal Autonomous Weapons Systems Deterrence." *JFQ: Joint Force Quarterly*, no. 110: 16–25. https://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=164969725&site=eds-live.

Sauer, Frank. 2022. "Lethal Autonomous Weapons Systems." PDF. In *The Routledge Social Science Handbook of AI*, edited by Anthony Elliott, 237–50. Routledge. https://cloudflare-ipfs.com/ipfs/bafykbzacecpxjtadxyj4h6sijw4qel55v5cayvdl77v3z3mzvbnhrwiyvd57i?filename=Anthony%20Elliott%20-%20The%20Routledge%20Social%20Science%20Handbook%20of%20AI-Routledge%20%282021%29.pdf.

Sayler, Kelley M. 2020. “Artificial Intelligence and National Security.” R45178. *Congressional Research Service*. Congressional Research Services. https://sgp.fas.org/crs/natsec/R45178.pdf.

Scharre, Paul. 2021. “Debunking the AI Arms Race Theory (Summer 2021).” *Texas National Security Review* 4 (3): 122–32. https://repositories.lib.utexas.edu/handle/2152/87035.

———. 2023. *Four Battlegrounds: Power in the Age of Artificial Intelligence*. W. W. Norton & Company.

Strayer, Rob. 2023. “Written Testimony of Rob Strayer for the Hearing on the Need for Transparency in Artificial Intelligence.” Testimony before the U.S. Senate Committee on Commerce, Science, & Technology. 118th Cong., September 12. https://www.commerce.senate.gov/services/files/6411107B-1128-40A8-9446-E342A83CF5E0.

Tallberg, Jonas, Eva Erman, Markus Furendal, Johannes Geith, Mark Klamberg, and Magnus Lundgren. 2023. “The Global Governance of Artificial Intelligence: Next Steps for Empirical and Normative Research.” *International Studies Review* 25 (3). https://academic.oup.com/isr/article/doi/10.1093/isr/viad040/7259354.

United Nations. 2023. “First Committee Approves New Resolution on Lethal Autonomous Weapons, as Speaker Warns ‘An Algorithm Must Not Be in Full Control of Decisions Involving Killing’ | Meetings Coverage and Press Releases.” November 1, 2023. https://press.un.org/en/2023/gadis3731.doc.htm.

———. n.d. “Lethal Autonomous Weapon Systems (LAWS) – UNODA.” Accessed May 3, 2024. https://disarmament.unoda.org/the-convention-on-certain-conventional-weapons/background-on-laws-in-the-ccw/.