OUR SECURE FUTURE

Women Make the Difference

Women, Peace and Security and Technology Futures:

What World Are We Building?

By Sahana Dharmapuri and Jolynn Shoemaker

OUR SECURE FUTURE

ABOUT THE AUTHORS

Sahana Dharmapuri

Ms. Dharmapuri has over two decades of experience in the public policy and human rights advocacy arena, with a primary focus on women's rights. She is one of a small number of people in the world with deep expertise on Women, Peace and Security. She advises the USG (mainly the Department of Defense, Department of State and Congress), NGOs, international bodies, foreign governments and militaries on how to address women's rights pragmatically and effectively. Ms. Dharmapuri is the Vice President of Our Secure Future and Vice President of the PAX *sapiens* Foundation.

Jolynn Shoemaker

Ms. Shoemaker is a Fellow at Our Secure Future and has over two decades of experience in international peace and security across government, academia, think tanks and non-governmental organizations. She has worked with numerous organizations engaged in policy-relevant strategy, research, advocacy and training on Women, Peace and Security and women's leadership. Previously, she worked at the U.S. Department of State and Department of Defense in policy and legal positions. Ms. Shoemaker is the Senior Director of Global Engagements in Global Affairs at the University of California, Davis.

Acknowledgements

Thank you to Yulia Shalomov, Emma Boggess and Mary Peplinski of Our Secure Future for their time and support in producing this report.

TABLE OF CONTENTS

I. INTRODUCTION

In science fiction movies, there is usually a critical moment that determines the future course for humanity. Often this leads to heroic efforts to avoid a dystopian, nightmarish future. In our real world, we have no way of knowing what the future may hold, but the recognition is rapidly setting in that technology, including Artificial Intelligence (AI) and future innovations, will reshape the world. These technologies will have profound effects on peace and security.

This raises some fundamental questions for the future of humanity:

What kind of world are we creating with emerging technologies?

Who is making decisions about what that world will look like?

Who will be more, or less, secure in this new world?

These questions are critically important for international peace and security but are being brushed aside in the current geopolitical technology race. Technology is increasingly intertwined with both American military strength and economic power. The dynamic evolution of AI has created motivations to accelerate the design process and to apply new technologies for strategic advantage as quickly as possible. However, when it comes to peace and security, policymaking that focuses on short-term advantages often leads to long-term, unintended consequences – especially for civilians and those disproportionately affected by instability. Women and girls in particular are among the first to experience the warning signs. Those signs have already started to manifest with technologies that are increasingly weaponized against women and girls.

At the same time, the relationship between the government defense sector and the technology industry is growing stronger, as both sectors see mutual benefit from deepening ties. This raises concerns about the potential concentration of power

and wealth, as well as equitable representation in decisions that will have broad ramifications for people globally. The emerging ecosystem is effectively squeezing out civil society voices and de-prioritizing human rights and humanitarian law. This shift affects policy decisions on technology, leading to critical blind spots and reshaping the future of peace and security.

The Women, Peace and Security (WPS) agenda is a framework aimed at supporting long-term security, particularly relevant in the context of emerging technologies. This commitment is both a bipartisan-supported law in the United States and a global mandate. This agenda uses a systems-based approach to investigate the root causes of instability and the necessary conditions for peace. It consequently provides a necessary framework to understand and address the increasing weaponization of technology, its impact on decision-making, access to resources and power dynamics and its overall effect on collective security.

About this Project

This white paper is a first step in integrating Women, Peace and Security into technology and security decisions. As part of a long-term Our Secure Future (OSF) project, it aims to assess the digital ecosystem's different impacts on men, women, boys and girls and apply established Women, Peace and Security principles to technology policy. The project explores the links between technology, women's participation and security, and seeks to improve strategic decisions regarding technology norms and policies.[1]

This white paper aims to foster a deeper understanding of the intersection between emerging technology and peace and security, and to highlight the importance of considering the long-term security implications of technology development and implementation from the second Obama Administration (2013-2017) to the current Trump Administration in 2025.

Methodology

This white paper primarily examines the evolving landscape of U.S. policymaking on technology and AI, with the recognition that there are many other relevant policy initiatives happening globally. The project draws upon two decades of Women, Peace and Security policy commitments and experiences worldwide to inform policy and advocacy on technology and security. The information presented here is based on an extensive review of policy trends and initiatives over several U.S. administrations, as well as interviews with over 40 individuals working at the intersections of technology and security and those with experience applying Women, Peace and Security objectives in diverse contexts around the world.

This paper does not attempt to catalogue every policy initiative related to technology, peace and security, as they are myriad examples from the U.S. Government and other institutions. The technology and security policy space is nascent and dynamic. Women remain underrepresented in technology decision-making, face unequal access to technology and are often victimized through digital platforms. Sometimes these issues have been recognized on an ad hoc basis by policymakers. Yet, these issues are rarely examined from a systems perspective or linked to peace and security outcomes. Women, Peace and Security is a useful lens for identifying remaining blind spots and for understanding and navigating these challenges effectively.

II. UNDERSTANDING THE RELEVANCE OF WOMEN, PEACE AND SECURITY FOR TECHNOLOGY POLICY

Women, Peace and Security (WPS) is an international commitment reflected in UN Security Council resolutions and domestic laws around the world.[2] In the international context, it builds upon decades of established international human rights, women's rights and humanitarian commitments. It is also a legal mandate in the United States. The 2017 *Women, Peace and Security Act* was signed into law by President Donald Trump with bipartisan support.[3] Over both Republican and Democratic administrations, U.S. Government agencies have developed subsequent strategies, plans, positions and initiatives to advance this agenda. Women, Peace and Security also continues to be reaffirmed as a commitment globally, including in the 2030 Agenda for Sustainable Development and the Pact for the Future.[4]

This commitment is supported by extensive evidence from contexts around the world, illustrating the impact of women's meaningful participation in—or their exclusion from—peace and security. Women and children bear the brunt of conflict and violence. Yet, women's perspectives, experiences and priorities are often missing from the decision-making processes that relate to peace and security. Women's organizations and civil society groups advocating for this agenda have called for meaningful involvement in security decisions that affect their lives, families, communities and countries. As technology reshapes the future of security, incorporating these perspectives is more crucial than ever, as the new emerging technology ecosystem risks being designed with incomplete information if it leaves out women.

Women, Peace, and Security is a transformative framework to understand the root causes of conflict and ensure women's comprehensive participation in decision-making processes related to peace and conflict. Women, Peace and Security is not only applicable to contexts of physical armed conflict. It also extends to the full range of peace and security issues, encompassing early warning and conflict prevention to long-term peace initiatives and democratic governance efforts. These areas are both influenced by and have an impact on emerging technologies.

Women, Peace and Security addresses four key thematic areas: (1) inclusion of women's perspectives in conflict prevention and early warning; (2) equal participation of women in peace processes and decision-making relating to peace and security; (3) protection and promotion of human rights for women and girls; and (4) equal access to relief and recovery. Technology can be weaponized in a number of ways that intersect with Women, Peace and Security. For example, biases and violence facilitated by technology can obstruct conflict prevention and the protection of women and children. Underrepresentation of

women in decision-making relating to technology, peace and security similarly sidelines women's perspectives and civil society participation.

Women, Peace and Security promotes deeper understanding of the multi-faceted challenges for peace and security in three ways: as a systems-level power analysis, as an early warning signal and as a call to action. Currently, these types of analyses and actions are missing from both policy and practice relating to technology, peace and security.

1. **An Early Warning Signal:** Women, Peace and Security recognizes that the marginalization and unequal status of women and girls is often a prelude to broader political and societal instability. Extensive research demonstrates the linkages between the treatment of women and the peacefulness of states.[5] Women, Peace and Security identifies root causes of insecurity and violence, recognizing that the widespread occurrence of such violence is more than a "women's issue," and rather an early warning sign of broader instability.

   In recent years, there has been some focus in the policymaking arena on how technological tools can provide advance warning of climate-related risks, humanitarian disasters and atrocities. However, there has been a missing connection between early warning research and practice from Women, Peace and Security, and its capacity to inform technology, peace and security policy. Recognizing the correlation between women's status and security is necessary to properly anticipate and prevent unintended consequences of technology design and deployment.

2. **A Call for Increasing Operational Effectiveness:** Women, Peace and Security is also a call to action, as all countries (including the U.S.) have agreed to this commitment. This agenda envisions increasing operational effectiveness in peace and security decision-making, including in complex security environments. Our Secure Future has documented examples of the value of applying Women, Peace and Security.[6] This agenda benefits all members of society by:

   - instituting more effective and democratic decision-making processes;
   - designing programs and policies backed by evidence and more nuanced and comprehensive information; and
   - addressing early warning signs that are identified by WPS analysis.

3. **A Systems-Level Power Analysis:** Lastly, Women, Peace and Security examines how decisions affect the peace and security of different segments of society.

   Women, Peace and Security analyzes the means by which women and girls are persistently marginalized and identifies where there are constraints and opportunities for transforming such forms of discrimination and marginalization.[7] This systems-level approach makes visible power dynamics, revealing who holds power and who is excluded from it. By applying a systems-level analysis, Women, Peace and Security is also meant to reveal blind spots and unforeseen consequences of security decisions for everyone.

   In the technology, peace and security area, this type of analysis can provide a better understanding of how the digital ecosystem is developing. Emerging technologies and surrounding questions – such as who has access, who is making decisions about design and use, who is vulnerable to abuse, who benefits and who is left out – all relate back to who holds power, with direct effects on peace and security.

III. THE EVOLUTION OF U.S. POLICYMAKING ON TECHNOLOGY, PEACE AND SECURITY

This project is based on an analysis of the technology, peace and security landscape over several U.S. administrations, from President Obama's second term to President Trump's second term in office. Overall, technology policy in the U.S. has been largely reactive and disjointed, as decision-makers face a quickly changing digital ecosystem. Silos across the U.S. Government have consequently reflected divergent priorities for technology policy.

A review of the national security policies between the second Obama Administration and the second Trump Administration highlights the rapid increase in attention on emerging technologies. The Obama Administration began to include cybersecurity as a key focus area of national security, passing an *Executive Order on Critical Infrastructure Cybersecurity* (2013), the *Cybersecurity National Action Plan* (2014) and the *Cybersecurity Information Sharing Act* (2015). In addition, the Obama Administration drastically expanded the use of unmanned aerial vehicles (drones) for targeted killing – policies that were controversial due to the civilian casualties reported by outside sources and secrecy surrounding their application. The increased use of drones served as a precursor to the integration of autonomous capabilities into warfare through other technologies, such as AI. The first Trump Administration continued the focus on cybersecurity, including with the *National Cyber Strategy* (2018). The Administration also made the connection between AI and national security with the *Executive Order on Maintaining American Leadership in Artificial Intelligence* (2019) and the establishment of the Joint Artificial Intelligence Center (2018). It furthermore focused on technological innovation with the private sector and increasing the speed of technology deployment.

Since the first Trump Administration, U.S. national security policy on technology has reflected a consistent focus on geopolitical and economic competition with China and leveraging technology for warfighting capabilities. This broad framing has changed very little across subsequent administrations. However, there have been major differences in approaches. The Biden Administration focused on the use of diplomacy and development for technology and democracy promotion, which was presented as an alternative to authoritarian models like that of the Chinese government. Issues related to gender equality in technology, bias, online violence and unequal access to technology were likewise highlighted. However, these policies were generally separate from defense and national security, where the emphasis remained on maintaining warfighting superiority. There were minimal connections to existing commitments such as Women, Peace and Security in various segments of the U.S.

Government. The Biden Administration formed a range of coalitions and partnerships with countries sharing similar values to advance new, shared principles. However, this seemed to reflect an ad hoc approach rather than a dedicated intent to build upon established international frameworks or multilateral mechanisms for dialogue and negotiation (e.g., the United Nations).

Early indications in the second Trump Administration suggest a focus on technology innovation and de-regulation, as well as rejection of the democracy and development priorities of the Biden Administration. This shift is particularly noticeable in the development of AI policy.

The policies of the Biden Administration attempted to cautiously balance the opportunities and risks of AI. In 2023, the White House released Executive Order 14110 - *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence,* which outlined eight guiding principles and priorities for the responsible development and use of AI.[8] The executive order (EO) also addressed concerns about bias, discrimination and inequalities that could be perpetuated through AI. In contrast, one of the initial actions of the second Trump Administration was the revocation of Executive Order on the *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023), deemed an impediment to innovation and U.S. leadership. The new Administration emphasized the necessity for the United States to act decisively to maintain global leadership in artificial intelligence. It also directed the government to develop a new action plan for AI within 180 days.[9]

In January 2025, the Trump Administration released Executive Order 14177 - *President's Council of Advisors on Science and Technology* establishing an advisory council on science and technology. The EO highlights the Administration's perspective on technology as a critical lever in geopolitical competition and U.S. national security: "*Today, a new frontier of scientific discovery lies before us, defined by transformative technologies such as artificial intelligence, quantum computing, and advanced biotechnology. Breakthroughs in these fields have the potential to reshape the global balance of power, spark entirely new industries, and revolutionize the way we live and work. As our global competitors race to exploit these technologies, it is a national security imperative for the United States to achieve and maintain unquestioned and unchallenged global technological dominance."*[10]

In May 2025, President Trump traveled to the Middle East with more than 30 business leaders, including from leading technology companies. A key focus of the visit was the sale of technology hardware and software (commercial and defense) and the development of AI data centers.[11] Earlier in May, the Trump Administration announced the cancellation of the *Framework for Artificial Intelligence Diffusion* (also known as the AI Diffusion Rule), established by the Biden Administration to control exports of AI hardware internationally.[12]

The increasing visibility of the technology industry in foreign policy and national security highlights the rise of technology companies as influential geopolitical actors.[13] This is matched by an acceleration of funding for emerging technology innovation that is bringing the U.S. Government, tech companies, venture capital and private equity firms closer together as global military expenditures continue to rise overall, with the U.S. spending more than any other country. The national security ecosystem is moving to accommodate billions of dollars of contracts with tech companies and smaller start-ups. For example, defense tech startups received more than $100 billion in venture capital funding between 2021 and 2023.[14]

Tech companies are, in turn, shifting their institutional priorities and principles to better position for national security business opportunities.[15] The revision in Google's AI principles to better facilitate defense contracts is illustrative of this trend. In 2018, responding

to protests from thousands of employees over a Department of Defense (DoD)* contract that would have utilized Google AI technology to analyze drone surveillance, Google released a set of AI principles that reflected a refusal to develop technologies that: could cause harm or injury to people, would use surveillance in violation of international norms or would fail to comply with international law and human rights.

In February 2025, Google updated its principles, with a different focus on "bold innovation, responsible development and deployment, and collaborative progress together."[16] These new principles include a reference to "widely accepted principles of international law and human rights," and identify industry, academia, governments and civil society as partners for collaboration. However, they noticeably make no commitment to exclude the development of AI that can be weaponized, used for surveillance or result in harm. Other tech companies, such as OpenAI, have followed suit, amending their principles to facilitate national security.[17] These shifts in principles have implications for the types of technologies that are developed and how potential risks for civilians are evaluated.

The U.S. military and the tech sector are also collaborating to innovate in such areas as quantum science and Artificial General Intelligence (AGI). In 2022, DoD established the Office of Strategic Capital to provide funding to industry partners for critical technology development and deployment.[18] AGI in particular is being eyed as a game changer for military dominance. Yet amid this growing alliance between the defense and tech sectors, there is little attention directed to the linkages between technology, instability and conflict, or its impact on human security. In a 2025 paper, for example, RAND identified national security problems that could emerge from AGI, including the proliferation of weapons and the development of a possible "wonder weapon" (a weapon that would create a transformative advantage in warfighting) and increased instability.[19]

Yet despite the uncertainties surrounding these emerging technologies, there has been no effort to apply a Women, Peace and Security lens to examine the risks and potential impacts for long-term peace and security.

The institutional entry points within the U.S. Government for applying the Women, Peace and Security framework to the future of war and conflict continued to shrink in 2025 with Trump Administration statements and plans. In April 2025, U.S. Secretary of Defense Pete Hegseth announced on social media that he had "ended" the Women, Peace and Security program in DoD. Secretary Hegseth indicated that the department would comply with only the minimal reporting requirements mandated by the *Women, Peace and Security Act* signed during the first Trump Administration.[20] Subsequent comments highlighted that the Administration disagreed with how the law had been interpreted and implemented by the previous administration. Meanwhile, the Department of State released a proposed restructuring plan that would eliminate the Office of Global Women's Issues, which had taken the lead on institutionalizing Women, Peace and Security across that department.

As the U.S. enters a new phase of national security that promotes unbridled innovation and U.S. technological dominance, Women, Peace and Security provides an important framework through which to assess the emerging landscape, identify existing blind spots and inform decision-making within both the defense and tech sectors. However, considering the current uncertainty about the future of Women, Peace and Security in the Departments of Defense and State, there will likely be additional obstacles in applying this agenda to emerging technology and national security policymaking.

*This paper uses the statutory designation "Department of Defense." In September 2025, President Donald Trump signed an executive order allowing the department to be referred to as the "Department of War" in certain contexts. However, statutory references to the Department of Defense and its officials remain unchanged unless modified by law.

IV. WHERE ARE THE STRATEGIC BLIND SPOTS IN TECHNOLOGY, PEACE AND SECURITY?

This project has identified three critical and strategic blind spots in the ongoing development of technology and AI through the lens of the Women, Peace and Security framework. These strategic blind spots prevent a systems-level approach to addressing technology opportunities and challenges for security. The blind spots impede conflict prevention, the protection of civilians (particularly women and children) and the participation of women as mandated by Women, Peace and Security. These issues have persisted across multiple U.S. administrations. While some of these blind spots have been mentioned in different U.S. administrations' technology policy discussions, the links to peace and security have frequently been overlooked.

Protection: The lack of comprehensive and nuanced analysis on the different impacts of technology on women, men, boys and girls negatively affects situational awareness and increases civilian vulnerability, which has implications for broader peace and security.

Prevention: The design of new technology and AI exacerbates the already existing inequalities between men, women, boys and girls. This inequality in the design and use of technology by men and women often provides early warning signals of broader insecurity. Yet, these weaknesses in developing technology and the ensuing security threats are often overlooked as indicators.

Participation: The universal right to fully participate in all forms of public life for men and women (recognized in international human rights instruments) is not considered in technology and AI security spaces. In addition, civil society is excluded from high-level policy and technology decisions, reducing understanding of long-term security effects.

Blind Spot 1: Protection

The lack of comprehensive and nuanced analysis on the different impacts of technology on women, men, boys and girls negatively affects situational awareness and increases civilian vulnerability, which has implications for broader peace and security.

The futurist Amy Webb has argued, "in the future, wars will be fought by code."[21] In recent years, cyberattacks by both state and non-state actors have demonstrated that many conflicts of the future will occur in the digital realm, with potentially catastrophic impact on infrastructure, financial systems and communications. Advances in AI are already re-shaping militaries and their operations on the ground in fundamental ways. Technology is now widely recognized within U.S. policymaking circles as a national security imperative and a critical lever in strategic competition against China.[22] This has pushed forward a dominant narrative that the U.S. needs to develop and deploy technology for military applications as quickly as possible.

This is apparent in the new structures established within DoD within the last five years. In 2021, DoD created the Rapid Defense Experimentation Reserve to support rapid experimentation with emerging technologies for warfighting. In 2023, DoD launched the Replicator Initiative, which was developed to accelerate the acquisition process for commercial technologies that can be taken to the battlefield.[23] The initiative's first phase focused on the acquisition of autonomous systems, including autonomous drones across multiple domains within 24 months of launch. According to DoD's Defense Innovation Unit, "Replicator is strengthening collaboration between DoD and the commercial technology sector. More than 500 companies have participated in Replicator-1 through a variety of onramps including the Commercial Solutions Openings, and more than 30 have received contracts, supported by over 50 major subcontractors. About 75% of the companies currently involved in supplying Replicator-1 capabilities are non-traditional defense contractors."[24]

However, there are several inherent risks in accelerating the acquisition process to implement emerging technologies such as AI to security contexts. The focus on speed and innovation may lead to the premature deployment of emerging technologies before they have been fully evaluated. Inadequate consideration of safety considerations and design flaws are more difficult to address after systems are deployed. Unfortunately, the main purpose of these innovations is lethality, not peace. One question that has not received adequate attention in the national security arena is the possible impact of accelerating acquisition processes for civilians, including for women and children, as well as non-combatants on the ground.

The Dangers of Premature Technologies for Accurate Situational Awareness

Premature deployment of technologies can impede situational awareness in unstable and violent environments. According to the Center for Naval Analysis, situational awareness is "the result of a dynamic process of perceiving and comprehending events in one's environment, leading to reasonable projections as to possible ways that environment may change, and permitting predictions as to what the outcomes will be in terms of performing one's mission. In effect, it is the development of a dynamic mental model of one's environment."[25] Some of the most critical challenges with the deployment of AI in conflict zones relate to insufficient or faulty training data, hallucinations, lack of transparency and compressed decision timelines.[26]

The UN Institute for Disarmament Research has noted in a report on AI military bias, "Data training sets can be flawed due to incomplete data, low-quality data, incorrect or false data, or discrepant data. These limitations are all at play, often in overlapping ways, in considerations of gender and machine learning." The publication points out that reliance on data from the Internet is not representative of women and girls, as they often remain disconnected from technology tools and platforms.[27]

One related danger is the presentation of factually incorrect information, or AI "hallucinations." There has been a documented increase in errors in new AI reasoning systems; hallucination rates on newer AI systems have doubled in some cases for companies. This can be further compounded when AI systems hallucinate at each step in a process.[28] Furthermore, the development of synthetic data by AI systems has also resulted in "intersectional hallucinations," as highlighted in an experiment with synthetic data, gender and population data.[29] As this research demonstrates, data sets need to be examined more carefully, especially as the use of synthetic data to train machine learning models increases.

The complexity of making decisions about civilian-combatant distinctions in the fog of war is of particular concern with AI systems. Bias – in both human judgment and machine identification – needs to be adequately understood and addressed before more advanced and more lethal systems are used on the battlefield.[30] AI systems and the advent of AGI create a "black box" problem, as it becomes more difficult to understand how the systems reach conclusions and make decisions. AI systems inherently lack transparency in these processes. In conflict environments, there is also pressure for quick decision-making. This can contribute to over-confidence and over-reliance in AI assessments and recommendations. Military analysts have pointed to the importance of retaining human judgement in conflict situations and how AI might erode that in dynamic warfare environments.[31]

The history of using drones in combat shows some of the risks to situational awareness and protection of civilians that could be amplified with more reliance on AI. In 2021, a major investigation by the *New York Times* uncovered repeated mistakes in drone attacks that led to the deaths of civilians. The reporting showed that "ordinary citizens were routinely mistaken for combatants," and that decision-makers often exhibited "confirmation bias" that led them to make faulty decisions about targeting. [32]

The complexity of making decisions about civilian-combatant distinctions in the fog of war is of particular concern with AI systems. Bias – in both human judgment and machine identification – needs to be adequately understood and addressed before more advanced and more lethal systems are used on the battlefield.

The Problems with Technologies and Targeting

A briefing paper submitted to the Convention on Certain Conventional Weapons (CCW) states that "situational awareness as a prerequisite for the identification and selection of legitimate targets (what has been named the Principle of Distinction) is not translatable into machine executable code. Yet situational awareness is essential for adherence to International Humanitarian Law (IHL) or any other form of legally accountable rules of conduct in armed conflict."[33]

Do emerging AI systems have the capacity to distinguish combatants from civilians amid the uncertain conditions in war and the pressure to make rapid decisions? Furthermore, what are the

implications of targeting mistakes on adherence to IHL, human rights obligations and laws such as the *Women, Peace and Security Act*?

The United Nations Institute for Disarmament Research (UNIDIR) has highlighted potential problems with AI systems correctly distinguishing combatants and civilians: *"The criteria that will inform who is and is not a combatant – and, therefore, a target – will be likely to involve gender, age, race and ability. Assumptions about men's roles, for example, may mis-categorize civilian men as combatants due to encoded gender biases among human operators as well as within the data-driven process itself."*[34]

The issues around data sets and targeting raise significant concerns as security actors increasingly seek to deploy autonomous weapons. Civil society organizations working on gender equality have been on the forefront of mobilizing discussions on the future of autonomous weapons systems that utilize emerging technologies. Women's International League for Peace and Freedom (WILPF) is part of an international civil society-led movement to ban lethal autonomous weapons systems (LAWS). The *Campaign to Stop Killer Robots* is a coalition of 250 organizations in 70 countries that are pushing for a treaty on autonomous weapons.[35]

According to WILPF: "*Autonomous weapon systems cannot be relied upon to comply with international humanitarian law or human rights. Robots programmed to kill might accidentally kill civilians by misinterpreting data. They would also lack the human judgment necessary to evaluate the proportionality of an attack, distinguish civilian from combatant, and abide by other core principles of the laws of war. Many tech workers, roboticists, and legal scholars believe that we will never be able to programme robots to accurately and consistently discriminate between soldiers and civilians in times of conflict."*[36]

The conflicts in Ukraine and Gaza have become testing grounds for emerging commercial technology in warfare, specifically in targeting and autonomous drones. In both the Ukraine and Gaza cases, U.S. tech companies have sold AI and cloud computing technologies for use in the war, including targeting and facial recognition software. Civil society groups have warned that unchecked usage of these types of technology tools in war can set the stage for abuses.[37]

In Gaza, Israel has deployed systems called Gospel (which marks buildings and structures) and Lavender (which marks individuals) to help identify targets for strikes. According to media reporting, Lavender has a misidentification rate of 10 percent. *Associated Press* reporting has linked AI with civilian deaths.[38]

The emerging landscape for AI and armed conflict necessitates an analysis that takes into account the different inequalities facing women, men, boys and girls. The *Women's Entrepreneurship and Economic Empowerment Act* (2018) offers a definition for gender analysis as a mechanism to address the structural inequalities that prevent all people from fully participating and enjoying the benefits and opportunities in society.[39] This type of analysis helps to answer two key questions: who is represented in the data that informs an understanding of the environment, and who is being left out. The implementation of gender analysis through the Women, Peace and Security framework would illuminate important social, economic and political aspects of the environment, supporting situational awareness and informed decision-making.

REGULATING LETHAL AUTONOMOUS WEAPONS SYSTEMS

In the U.S. there is no legislation that prohibits the development or use of semi-autonomous and autonomous weapons. U.S. guidance on LAWS is articulated in DoD Directive 3000.09 (updated by DoD in January 2023). It provides that "Autonomous and semi-autonomous weapon systems will be designed to allow commanders and operators to exercise appropriate levels of human judgment over the use of force." The updated directive further states that "Persons who authorize the use of, direct the use of, or operate autonomous and semiautonomous weapon systems will do so with appropriate care and in accordance with the law of war, applicable treaties, weapon system safety rules, and applicable rules of engagement (ROE). The use of AI capabilities in autonomous or semi-autonomous weapons systems will be consistent with the DoD AI Ethical Principles, as provided in Paragraph 1.2.f."[40]

The Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons Which May Be Deemed to Be Excessively Injurious or to Have Indiscriminate Effects (CCW) is one mechanism that could address LAWS internationally. CCW integrates international humanitarian law and its structure enables new types of technologies to be added. The CCW process also allows the inclusion of civil society stakeholders, not only UN member states.[41]

The U.S. has participated in the CCW discussions on LAWS since 2014, with the position that LAWS can be adequately addressed with existing international humanitarian law. Thus far, the CCW meetings on LAWS have focused on developing a set of guiding principles that are rooted in international law, specifically international humanitarian law, but no concrete recommendations have been made on the restriction or prohibition of these types of weapons.

In 2024, a UN General Assembly First Committee resolution stated, "that a comprehensive and inclusive approach will be required to address the full range of challenges and concerns posed by autonomous weapons systems, including consideration of legal, technological, ethical, humanitarian and security perspectives, in order to safeguard international peace and security."[42] The resolution also included a decision to open informal consultations in 2025 that will be open to governments, regional and international organizations and civil society. The UN report, *Governing AI for Humanity* (2024), states, "Presently, 120 Member States support a new treaty on autonomous weapons, and both the Secretary-General and the President of the International Committee of the Red Cross have called for such treaty negotiations to be completed by 2026. The Advisory Body urges Member States to follow up on this call."[43]

Blind Spot 2: Prevention

The design and use of new technology exacerbate the already existing inequality between men and women and therefore misses the critical early warning signal that women and girls' experiences in insecure environments indicate. Women and girls' insecurity, whether in a conflict environment, unstable complex emergency or stable society, often signals broader risks and threats to security. Yet biases between and among men, women, boys and girls are often overlooked by security actors as early warning indicators for peace and security. This bias is now embedded in the technology that security actors rely on to make decisions.

In the years since Women, Peace and Security was adopted internationally, substantial research and practice have demonstrated correlations between women's security and security within and among countries.[44] The mistreatment of women and girls is often one of the first signs of systemic problems and has been shown repeatedly to be a root cause of broader instability. This pattern has been documented extensively across countries and contexts.[45]

In its publication, *Gender and Early Warning Systems,* the OSCE Office for Democratic Institutions and Human Rights (ODIHR) underscored the importance of incorporating a gender perspective in early warning systems: "*By bringing to light such patterns of structural discrimination, integrating a gender perspective can improve the effectiveness of early warning systems by gathering more specific information and allowing for more detailed and precise analysis. In turn, this can ensure better preparedness and, when necessary, more accurate and measurable responses — as well as preventive mechanisms — that can more directly address some of the underlying causes of a conflict."*[46]

The mistreatment of women and girls is often one of the first signs of systemic problems and has been shown repeatedly to be a root cause of broader instability.

The report goes on to note that this kind of social and power analysis highlights factors relating to women's rights that have effects on security, and that women are often the first to experience weakened security.

Policymakers increasingly recognize that state and non-state actors utilize technology to restrict civic space, control information and target political opponents and civil society actors. These activities are often intended to destabilize society or government, solidify political and economic power or bolster anti-democratic interests. Technological tools and platforms often support tactics that create instability, such as:

- Online violence, harassment and discrimination
- Mass surveillance
- Censorship
- Disinformation and misinformation
- Biased data and exploitation of digital data
- Cybersecurity attacks, including those directed at civil society

Many of these threats are interconnected with gender. According to UN Women, "technology-facilitated gender-based violence"[47] (TFGBV) is an act that uses technology to cause harm to women, girls and LGBTQI people. Instances of TFGBV have been documented globally. Violence on technological platforms is increasingly translating into physical violence. Doxing, online bullying, cyberstalking and online harassment are just a few examples with real-world consequences.

While there has been some acknowledgement of the impact of this on democracy, it is equally important to understand the implications for the peace and security and how the treatment of women online can serve as an indicator of violence and broader insecurity.

Both state and non-state actors utilize technology and technological platforms to promote misogynistic tactics for authoritarian agendas. Female civil society leaders and political activists are deliberately targeted through these tactics. Such actions cause a chilling effect on the social, political or economic participation of women and other groups online and are often associated with physical violence.

According to reporting by the Economist Intelligence Unit, the global prevalence of online violence against women is 85 percent.[48] A report from the Georgetown Institute for Women, Peace and Security also found that TFGBV serves as a key driver of radicalization and violent extremism.[49] In Myanmar, for example, online extremist content promoted sexual and gender-based violence against women and girls during the military coup.[50]

G*endered Disinformation: Tactics, Themes, and Trends by Foreign Malign Actors,* a bulletin produced by the U.S. Department of State,[51] referenced a multi-country study conducted by the United States, Canada, the European External Action Service (EEAS), Germany, Slovakia and the United Kingdom which highlighted the effects of gendered disinformation on governance: *"Our research underscores the importance of using a gender and identity-based lens to analyze the tactics used by foreign state and non-state actors to spread gendered disinformation that deliberately polarizes attitudes, sows division, and undermines social cohesion. The spread of gendered disinformation harms not only the targeted individuals, but also democracy."*[52] The report found that disinformation strategically targets women and people with intersecting identities to discourage freedom of expression and to undermine democracy. The effects of such tactics on health, justice and democracy are gaining increasing attention, yet the direct links with peace and security are often missing.

The Biden Administration launched several initiatives to address gender-based violence in technology, including the *Global Partnership for Action on Gender-Based Online Harassment and Abuse* and the *Global Call to Action to Address Technology-facilitated Gender-Based Violence.* Yet such activities were never explicitly connected with policy related to technology, peace and security, especially in the national security domain.

The U.S. Department of Homeland Security's Science & Technology (S&T) Directorate issued two grant awards in 2023 to examine GBV, including online threats, as a risk factor for targeted violence.[53] This included threats of online harassment and abuse and GBV as indicators of violence. While promising steps to begin connecting the experiences of women and girls online with broader instability, they were ultimately ad hoc and limited in scope. A comprehensive application of a Women, Peace and Security lens can help to illuminate the connections of these online dynamics with overall peace and security.

Examples of AI Use to Threaten Women's Participation and Safety

Advances in AI, in particular, can facilitate harms for women, children and other marginalized groups based on how it is developed, trained and deployed. Below are a few sample areas in which AI could be used to minimize women's participation and threaten their safety, with ripple effects for social stability and peace.

Bias in Data Sets

There is growing recognition of the dangers of inherent bias and discriminatory recommendations by technologies, especially AI systems. Many of these biases can be traced to the training data used for machine learning, as well as many other stages throughout AI development and deployment processes. Numerous cases have emerged from the private sector demonstrating how biases in training data can influence decisions, including the discriminatory effects of deploying AI in recruitment processes.

One of the most notable examples was Amazon's use of AI to support hiring decisions in 2014. Amazon used a decade of resumes and hiring decisions to train a machine learning system that would facilitate an automated resume screening process. According to media coverage of the story, because women were underrepresented in the dataset of job applicants used, Amazon's machine learning system penalized resumes that included the word "women's" or referenced all-women's colleges, rewarding instead resumes that used verbs more commonly found on male resumes. The inherent gender biases could not be fixed; Amazon abandoned the project in 2017.[54]

In 2020, MIT and NYU took down a data set called *80 Million Tiny Images* after a study found that it contained sexist and racist labels, as well as pornographic, non-consensual images of women. By the time it was taken down, the data set had been used and cited for 14 years.[55] A study of online images also showed that gender bias arises more frequently in images than text, and that images exacerbate the underrepresentation of women online.[56]

Other elements of machine learning, in addition to training data, can result in bias. The way that a problem is framed by the system's designers, the objectives designers set for the system's decision making and the attributes that are considered or ignored can all skew machine learning systems to find the most efficient way to achieve results — often in a discriminatory way.[57]

In the national security realm, AI is increasingly employed to support various tasks, ranging from identifying threats and sifting through immense amounts of data, to collecting and analyzing intelligence and determining targets. Biases in AI can have serious consequences for civilians including women, children and other marginalized communities. These actions could result in violations of rights, the implementation of unfair or discriminatory practices, incorrect predictions and the wrongful targeting of innocent individuals.[58]

Facial Recognition

Female experts in the technology space were some of the first to identify the now well-recognized facial recognition problems within many AI systems, and to research their broad consequences for society. Joy Buolamwini is the lead author of one of the most influential studies on AI gender and racial bias, *The Gender Shades Project*. This project explored the gender classification systems of three major corporations and found that AI systems were more accurate in identifying male faces than female faces. This difficulty was amplified with racial differences. The findings showed that "darker skinned females are the most misclassified group (with error rates of up to 34.7%). The maximum error rate for lighter skinned males is 0.8%."[59]

These embedded gender and racial biases and mistakes have significant repercussions for national security – misuse and errors in facial recognition technologies can threaten human rights and protections of civilians, especially those from marginalized groups. The technologies affect how security actors (e.g., military, police, etc.) collect, analyze and make decisions about threats. They can also be utilized by bad actors to promote their agendas through discrimination and abuse. The technologies are used by authoritarian regimes for mass surveillance and to suppress dissent by civil society and political opposition, as well as to target marginalized groups. One of the most significant dangers is that these AI systems can identify innocent individuals, neighborhoods or communities as threats.[60] In addition, the increasing use of these technologies despite the tendency of these systems to misidentify Black, Indigenous and people of color (BIPOC), both by the U.S. military and domestic law enforcement, raise both ethical and security concerns.[61] In counter-terrorism activities, there has often been the assumption that men and boys are the perpetrators of violence. These gender-based assumptions can also influence how technology tools, such as AI, analyze data, make predictions and shape recommendations for security actors.[62]

Deep Fakes

Deep fakes – or the application of AI technology to create someone's likeness in fake images, audio or video – is a growing phenomenon that disproportionately affects women and girls. Often, women who are public figures are targeted for deep fakes as a means of spreading disinformation, silencing women and chilling their participation in political processes. As with other threats that disproportionately affect women and girls, technology platforms and governments alike have been extremely slow to respond. Although the weaponization of this technology was first used by actors to target women, the connections with broader security were overlooked.[63]

In recent years, deep fakes have gained attention as a national security threat. For example, in 2022, a deep fake circulated on social media showing the Ukrainian president directing Ukrainian soldiers to surrender to Russian forces. Although this specific deep fake was a video of poor quality, it demonstrated how emerging technologies that are easily accessible can be used for information warfare. As technology reaches new levels of sophistication, foreign adversaries and non-state actors are likely to employ these tools to spread misinformation, destabilize political systems and instigate violence and social instability.

Technology companies are working on ways to address the growing threat with deepfake detection systems.[64] However, a study from the University of Southern California showed that the training data that is used for these detection systems may also reflect gender and racial biases. The study found that the facial profiles of Asian and African females are more likely to be mistakenly labeled as fake than the profiles of male Caucasians.[65]

In May 2025, President Trump signed the bipartisan *TAKE IT DOWN Act*, which "prohibits the nonconsensual online publication of intimate visual depictions of individuals, both authentic and computer-generated, and requires certain online platforms to promptly remove such depictions upon receiving notice of their existence."[66]

The legislation indicates that policymakers are increasingly aware of the significant risks deep fakes pose to individuals. Currently, the focus remains largely on protecting women and children from exploitation. However, there is a lack of comprehensive attention to the relationship between harms directed at women and children and the subsequent adoption of these technologies in broader security contexts. It is essential to assess how the targeting of women and children functions as an early warning indicator.

Blind Spot 3: Participation

High-level policy and technology decisions lack a comprehensive and nuanced understanding of long-term security effects because of the absence of participation and data gathering from civil society voices.

Civil society has been increasingly sidelined from policy discussions on emerging technologies, peace and security, which remain overwhelmingly insular and compartmentalized. Efforts to address technology and communities of practice are divided into issue-area silos – such as AI or cybersecurity. Viewing the issues in narrow silos has exacerbated the lack of policy cohesion across the technology and security domain. At the same time, a focus on government and private sector leadership has marginalized external civil society actors. This situation is further compounded by frequently evolving policy terminology concerning technology-related peace and security matters, which tends to exclude all but those considered insiders.

Official policy documents often only specifically mention government and industry actors, and to some extent academia/research. For example, the *DoD Responsible AI (RAI) Strategy and Implementation Pathway* includes a line of effort to "Integrate RAI as an Element of International Engagements to Advance Shared Values, Lessons Learned and Best Practices, and Interoperability Globally (LOE 5.3)."[67] Following this, there is an action item to "Organize a workshop with representatives from the international community (academia, industry and government) on AI ethics, safety and trust in defense in order to exchange best practices and promote shared values."[68] Broader civil society is notably not acknowledged as a relevant actor in such discourse. Other policy documents at times mention civil society and international collaboration, but there are insufficient mechanisms in place for meaningful participation of non-governmental, non-technical or non-industry stakeholders.

Civil society is most often acknowledged for innovations around technology, peacebuilding and democracy. Indeed, civil society actors are utilizing current technology to create new and creative mechanisms for civil engagement and to oppose authoritarian and extremist political forces. For example, civil society organizations have used technology platforms to promote government accountability, address corruption and advance peacebuilding in varied contexts ranging from Africa, the Middle East and the U.S.[69] These are important efforts to leverage technology for peace and democracy. But the recognition and inclusion of civil society is not translating into technology and national security policymaking.

A key challenge for civil society organizations is navigating the complex (and frequently changing) web of U.S. policy pronouncements, mandates, reports and bodies that are influencing national security and technology policy. Absent clear entry points to bring these voices and perspectives into policy debates, it is imperative for international and domestic civil society actors to form more influential coalitions to influence policymaking.

At the same time, policy actors also have a responsibility to ensure that civil society remains a central player in processes that will determine the future of technology, peace and security. Women, Peace and Security requires this inclusion. The lack of attention on civil society and women's organizations as critical actors in security and technology stands in stark contrast to U.S. Government commitments to Women, Peace and Security. The July 2022 *U.S. Government Women, Peace and Security Congressional Report* emphasizes the importance of these groups as key partners in peace and security.[70] The Department of State and Department of Homeland Security also mentioned specific examples of engagement.

The Women, Peace and Security agenda is centered on full participation of all stakeholders in peace and security. UN Security Council

Resolution 1325 on Women, Peace and Security came to pass because of the persistent efforts by civil society and women's organizations in countries experiencing instability to demand that their voices were heard.[71] The *Women, Peace and Security Act* and the National Action Plans on Women, Peace and Security passed in more than 100 countries are a direct result of this worldwide civil society advocacy. Civil society continues to function as an essential sector to ensure government accountability for this mandate, and other human rights and equality commitments.

Research from around the world on peace processes shows that women's engagement leads to more attention on the root causes of instability and violence and broadens the scope of policy issues and impacts that are considered by policymakers.[72] There are two decades of history in advancing Women, Peace and Security lessons and models for government and multilateral support for civil society engagement in peace and security. Equal participation of women and established mechanisms for regular consultations are key components for the involvement of all stakeholders. The failure to open the policy aperture to include civil society stakeholders and Women, Peace and Security analysis in national security discussions on technology presents a critical blind spot that has negative consequences for democratic governance and civic participation in one of the most consequential peace and security topics of our time.

Research from around the world on peace processes shows that women's engagement leads to more attention on the root causes of instability and violence.

V. CONCLUSION

As this report makes clear, there are significant risks associated with emerging technologies, peace and security. The report makes the case for grounding technological innovation and governance in international law, human rights and global commitments, including the UN Charter, human rights law and the 2030 Agenda for Sustainable Development, and the extensive commitments relating to Women, Peace and Security.

At the multilateral level, there are recent efforts to develop AI governance that reflect global commitments, and these may create new entry points for Women, Peace and Security. In September 2024, the UN Secretary-General High-Level Advisory Body on AI released a report, *Governing AI for Humanity*, which raises many questions that are consistent with Women, Peace and Security: specifically, who is benefiting from technology in wealth and power, and who is left out. Many recent technology governance efforts have not been truly global in reach. According to the UN report, they involve selective groups of governments, dominated by seven countries with more than 100 other countries left out.[73] Yet the implications of technology development and implementation will have profound impacts on all people and countries.

In January 2025, the UN established the Office for Digital and Emerging Technologies and in August 2025, the UN General Assembly (UNGA) adopted a resolution that set up the Independent International Scientific Panel on Artificial Intelligence and the Global Dialogue on Artificial Intelligence Governance – originally established in the Pact for the Future (2024). The new scientific panel will be comprised of 40 global experts responsible for producing an annual report on the risks, opportunities and impact of AI. The Global Dialogue on Artificial Intelligence Governance will involve both governments and relevant stakeholders as a platform to discuss international cooperation, share best practices and lessons learned and to facilitate open, transparent and inclusive discussions on artificial intelligence governance. Although human rights and international law are referenced directly, there is no direct reference to gender equality or Women, Peace and Security. These mechanisms may therefore provide opportunities for civil society engagement and advocacy for Women, Peace and Security considerations.

As the space for Women, Peace and Security within the U.S. Government continues to shrink, other governments that maintain a commitment to this agenda, along with civil society, private sector and academia, can play key roles in supporting technology governance that reflects shared principles and commitments. Global dialogues and forums that bring many stakeholders together can provide new mechanisms for participation and shaping the future uses of technology for the benefit of humanity.

Technology governance should be based on established international commitments, including Women, Peace and Security, and international human rights and humanitarian law principles. How emerging technologies affect women's treatment and participation needs to be a central consideration for the future of conflict and achieving long-term security.

VI. KEY FINDINGS

1. The U.S. Government does not directly address established international laws and commitments that promote peace and security in its consideration of emerging technologies. The focus on using these technologies in the race for economic and defense dominance has hindered meaningful policy discussion and alignment with international laws and norms.

2. Situational awareness is compromised by insufficient data collection from all groups within society, including men, women, boys and girls. Conventional security analysis methods that leave out technology's varied effects on women may negatively influence subsequent security plans, programs and activities. Technology-facilitated violence and embedded bias towards women and girls in technologies are indicators of systemic issues affecting national and international security.

3. New technologies are usually not designed with a human security perspective. The development and deployment of emerging technologies, such as autonomous weapons, in conflict zones pose specific risks to civilians, including women and children. The rapid acquisition and deployment of technologies in war raises concerns that civilian security considerations may be minimized.

4. Civil society voices, especially those with expertise in Women, Peace and Security, are not being included in technology, peace and security policymaking. Geopolitical competition and the military AI race and mixed policy objectives hinder civil society engagement. U.S. policy discussions on these topics remain insular, focusing primarily on government and private sector actors for the purpose of economic and military dominance.

VII. KEY RECOMMENDATIONS

Shed Light on the Blind Spots: Design Better Institutional Systems to Detect Strategic Blind Spots in Emerging Technologies.

- Create processes to assess new technologies applied to national security with a focus on civilian security, particularly for women and girls, and protecting human rights.
- Design peace and security early warning systems with indicators that assess women and girls' security and consider the impact of technologies on them.
- Integrate analysis tools and approaches that are informed by the Women, Peace and Security framework into programs and initiatives that relate to technology, peace and security.
- Ensure that diverse datasets are used to train AI systems in peace and security contexts. Develop algorithmic transparency and accountability measures that prioritize civilian security, with the participation of women and civil society. Improve data-sets based on a standard for data collection.
- Develop Women, Peace and Security-specific benchmarks: A benchmark is a curated suite of tasks and quantitative metrics designed to systematically evaluate how well an AI model handles a specific domain or capability. A Women, Peace and Security benchmark could evaluate AI tools used in peace and security contexts, revealing which AI models incorporate Women, Peace and Security data and perspectives. It consequently promotes accuracy and accountability in AI development.

Improve Security Decision-making: Expand the Talent Pool that Informs Security Analysis and Peace and Security Decision-making.

- Expand talent in technology and national security to include skills beyond STEM, such as Women, Peace and Security analysis and knowledge about international policy frameworks. These perspectives help predict long-term impacts of technology decisions on peace and security and prevent unintended consequences.
- Incorporate a wider range of expertise into technology, peace and security beyond government and the private sector, to include women's civil society organizations and leaders dedicated to Women, Peace, and Security, human rights, humanitarian protection and other issues that are central to civilian security and peacebuilding.

Strengthen Governance: Engage in consultative processes to address gaps in understanding how technology negatively affects women, girls, men and boys.

- Ensure that policy analysis and decisions on technology, peace and security are grounded in established U.S. law and international commitments that support women's rights. Policymaking documents and initiatives should explicitly incorporate Women, Peace and Security as a pertinent mandate for technology, peace and security.
- Address relevant issues around technology and conflict as part of the consultative and reporting mechanisms under the *Women, Peace and Security Act*.
- Incorporate technology issues into multilateral and civil society led Women, Peace and Security initiatives to enhance understanding of the impact of technologies on women and girls, drive more effective policy discussions and support technology governance aligned with women's rights and human rights.

ANNEX

Select U.S. Policy Documents with Relevance to Technology, Peace and Security

Since the Obama Administration, numerous reports, initiatives, policies and organizational changes have been introduced by the White House and relevant government agencies to address the evolving technology landscape. Prior to 2020, cybersecurity and the advancement of science and innovation received considerable attention, as evidenced in national security strategies and policy directives from both the Obama Administration and the first Trump Administration. During the Biden Administration and the second Trump Administration, emerging technologies became a central area of focus. The following examples (2020-2025) pertain to national security, diplomacy and development, reflecting a heightened emphasis on technology within the U.S. Government.

Note that this list does not encompass all U.S. policy documents related to technology.

Federal Laws & Congressional Mandates

National Artificial Intelligence Initiative Act (2020)

Established a coordinated federal approach to AI research, standards and workforce development.[74]

Chips and Science Act (2022)

Directed federal investment in AI, data science and cybersecurity research and workforce development.[75]

Executive Orders

Executive Order on the *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence* (2023)

This Biden Administration Executive Order was intended to regulate the use and development of AI safely and responsibly.[76] (In 2025, the Trump Administration rescinded this Executive Order.)

Executive Order on the *President's Council of Advisors on Science and Technology* (2025)

This Trump Administration Executive Order establishes an advisory council on science and technology to reinforce American leadership in science and technology.[77]

Executive Order on *Promoting the Export of the American AI Technology Stack* (2025)

This Executive Order is intended to boost global use of U.S. AI technologies and standards and decrease reliance on AI from adversarial nations.[78]

Executive Order on *Modernizing Defense Acquisitions and Spurring Innovation in the Defense Industrial Base* (2025)

This Executive Order aims to accelerate defense procurement and encourage technological innovation.[79]

U.S. Government Standards

AI Risk Management Framework | NIST (2023)

Provided guidance for managing risks and promoting trustworthy AI systems.[80]

U.S. Government Agency Initiatives

U.S. Department of Defense:

- **Department of Defense Digital Modernization Strategy**

  In 2019, DoD released its Digital Modernization Strategy. The Strategy presents a vision for "a more secure, coordinated, seamless, transparent, and cost-effective IT architecture that transforms data into actionable information and ensures dependable mission execution in the face of a persistent cyber threat."[81]

- **Department of Defense Ethical Principles for Artificial Intelligence**

  In 2020, DoD released five ethical principles to guide its use of artificial intelligence:

  1. Responsible. DoD personnel will exercise appropriate levels of judgment and care, while remaining responsible for the development, deployment, and use of AI capabilities.
  2. Equitable. The Department will take deliberate steps to minimize unintended bias in AI capabilities.
  3. Traceable. The Department's AI capabilities will be developed and deployed such that relevant personnel possess an appropriate understanding of the technology, development processes, and operational methods applicable to AI capabilities, including with transparent and auditable methodologies, data sources, and design procedure and documentation.
  4. Reliable. The Department's AI capabilities will have explicit, well-defined uses, and the safety, security, and effectiveness of such capabilities will be subject to testing and assurance within those defined uses across their entire life cycles.
  5. Governable. The Department will design and engineer AI capabilities to fulfill their intended functions while possessing the ability to detect and avoid unintended consequences, and the ability to disengage or deactivate deployed systems that demonstrate unintended behavior.[82]

- **Department of Defense Data Strategy**

  In 2020, DoD released its Data Strategy, which emphasizes the need to work closely with users in the operational community, particularly the warfighter. Initial areas of focus include: Joint All Domain Operations – using data for advantage on the battlefield; Senior Leader Decision Support – using data to improve DoD management; and Business Analytics – using data to drive informed decisions at all echelons.[83]

- **Department of Defense Responsible AI (RAI) Policy**

  In May 2021, the Secretary of Defense released a memo on Responsible AI (RAI), which included Responsible AI Ecosystem as one of the key tenets: *Build a robust national and global RAI ecosystem to improve intergovernmental, academic, industry, and stakeholder collaboration, including cooperation with allies and coalition partners, and to advance global norms grounded in shared values.*[84]

In June 2022, DoD published the Responsible Artificial Intelligence Strategy and Implementation Pathway, which also lays out specific lines of effort for DoD to implement the tenets of RAI. Although a number of U.S. legal sources are highlighted as foundational for AI ethics and RAI, including the Constitution, Title 10, the Law of War, privacy and civil liberties, and "long standing international norms and values," there is no further reference of U.S. legislation such as Women, Peace and Security that directly relates to the future of war and peace."[85] Civil society is mentioned briefly in the document, but the focus is on industry, academia and government as key stakeholders. Civil society engagement appears to be only considered within the public affairs and communications strategy, and the sector is not mentioned within consultation mechanisms that are outlined.[86]

- **Department of Defense Chief Digital Artificial Intelligence Office**

  In 2022, DoD established the Chief Digital Artificial Intelligence Office (CDAO) "to elevate digital and AI strategy development and policy formulation to the secretary and deputy secretary, while also ensuring unity of mission and tighter integration for the department's enterprise-wide data, AI, and cyber organizations."[87]

U.S. Department of State:

- **Department of State Cyberspace and Digital Policy Strategy**

  In 2022, the Department of State announced the establishment of a new Bureau of Cyberspace and Digital Policy. According to the Department website, "The Bureau addresses the national security challenges, economic opportunities and values considerations presented by cyberspace, digital technologies, and digital policy and promotes standards and norms that are fair, transparent and support our values."[88]

- **Political Declaration on Responsible Military Use of AI**

  The Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy provides a normative framework addressing the use of AI and automated capabilities in the military domain.[89] In February 2023, at the Responsible AI in the Military Domain Summit (REAIM 2023) in the Hague, the Declaration aims to establish international consensus around responsible behavior and guide states' development, deployment and use of military AI.

- **Enterprise Data and Artificial Intelligence Strategy**

  This strategy was released by Department of State in 2025 and aims to modernize diplomacy by using data and AI to improve operational efficiency, enhance decision-making and support strategic goals.[90]

U.S. Agency for International Development:

Previous to the Trump Administration, USAID released several key strategies relating to technology. Note that these documents are no longer available since the dismantling of this agency in 2025.

In 2020, USAID released a *Digital Strategy* for the period 2020-2024 to advance progress in communities in our partner countries.[91]

In 2022, USAID released an *Artificial Intelligence Action Plan*, which focused on both the benefits and risks of AI in development and promoted the idea of responsible AI.

Endnotes

1 Sahana Dharmapuri and Jolynn Shoemaker, "Women, Peace & Security, and the Digital Ecosystem: Five Emerging Trends in the Technology and Gender Policy Landscape," *Our Secure Future*, January 26, 2021, https://oursecurefuture.org/our-secure-future/publication/women-peace-security-and-digital-ecosystem-five-emerging-trends; Our Secure Future, "The Urgent Case for Gender Equality in the Digital Age," May 27, 2021, https://oursecurefuture.org/our-secure-future/publication/urgent-case-gender-equality-digital-age; Our Secure Future, "WPS Message Guide: A Gender Perspective on AI Risks to National Security," March 27, 2024, https://oursecurefuture.org/our-secure-future/publication/wps-message-guide-gender-perspective-ai-risks-national-security.

2 United Nations, "United Nations Security Council Resolutions on Women, Peace and Security," accessed February 24, 2025, https://www.un.org/shestandsforpeace/content/united-nations-security-council-resolutions-women-peace-and-security.

3 Congress.gov, "S.1141 – 115th Congress (2017–2018): Women, Peace, and Security Act of 2017," October 6, 2017, https://www.congress.gov/bill/115th-congress/senate-bill/1141.

4 United Nations, "UN Sustainable Development Goals," accessed February 27, 2025, https://sdgs.un.org/#goal_section; United Nations, "Pact for the Future, Global Digital Compact and Declaration on Future Generations: Summit of the Future Outcome Documents," September 2024, https://www.un.org/sites/un2.un.org/files/sotf-pact_for_the_future_adopted.pdf.

5 Valerie M. Hudson et al., "The Heart of the Matter: The Security of Women, the Security of States," *Army University Press*, June 2017, https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/May-June-2017/Hudson-Heart-of-the-Matter/.

6 Our Secure Future, "The Evidence for Women, Peace and Security," July 16, 2018, https://oursecurefuture.org/our-secure-future/news/evidence-women-peace-and-security#:~:text=to%20virtually%20zero.-,Peacebuilding%20and%20Conflict%20Resolution,negative%20impact%20on%20the%20process.

7 UN Women, "Guidance Note: Gender-Responsive Conflict Analysis," January 2022, https://www.unwomen.org/en/digital-library/publications/2022/03/guidance-note-gender-responsive-conflict-analysis.

8 Executive Order No. 14110, "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," The White House, October 30, 2023, https://www.federalregister.gov/documents/2023/11/01/2023-24283/safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence.

9 Executive Order No. 14179, "Removing Barriers to American Leadership in Artificial Intelligence," The White House, January 23, 2025, https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/.

10 Executive Order No. 14177, "President's Council of Advisors on Science and Technology," The White House, January 23, 2025, https://www.whitehouse.gov/presidential-actions/2025/01/presidents-council-of-advisors-on-science-and-technology/.

11 Juliana Liu, "On Middle East Tour, Trump Touts US Tech to Power Post-Oil Future," *CNN*, May 14, 2025, https://www.cnn.com/2025/05/14/tech/us-ai-chips-trump-saudi-arabia-visit-intl-hnk; Sara Dorn, "U.S. Will Build Massive AI Data Center in Abu Dhabi: See the List of Deals Trump Announced in the Middle East," *Forbes*, May 15, 2025, https://www.forbes.com/sites/saradorn/2025/05/15/us-will-build-massive-ai-data-center-in-abu-dhabi-see-the-list-of-deals-trump-announced-in-the-middle-east/.

12 Roberto J. González, "How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex," *Costs of War*, Watson Institute for International and Public Affairs, Brown University, April 2024, https://home.watson.brown.edu/research/research-briefs/transforming-military-industrial-complex.

13 Stockholm International Peace Research Institute (SIPRI), SIPRI Yearbook 2024: Summary, June 2024, https://www.sipri.org/sites/default/files/2024-06/yb24_summary_en_2_1.pdf; Audrey Kurth Cronin, "How Private Tech Companies Are Reshaping Great Power Competition," *Kissinger Center Papers*, Henry A. Kissinger Center for Global Affairs, Johns Hopkins School of Advanced and International Studies, August 2023, https://mediahost.sais-jhu.edu/saismedia/media/web/files/kissinger/how-private-tech-companies-are-reshaping-great-power.pdf; Katja Bego, "Silicon Valley's National Security Pivot Will Only Accelerate Under the New Trump Administration," *Chatham House*, November 29, 2024, https://www.chathamhouse.org/2024/11/silicon-valleys-national-security-pivot-will-only-accelerate-under-new-trump-administration; Liu, "On Middle East Tour, Trump Touts US Tech to Power Post-Oil Future

14 González, "How Big Tech and Silicon Valley Are Transforming the Military-Industrial Complex."

15 Bego, "Silicon Valley's National Security Pivot Will Only Accelerate Under the New Trump Administration."

16 Google, "AI Principles," last updated February, 2025, https://www.ai.google/responsibility/principles/; Scott Shane and Daisuke Wakabayashi, "'The Business of War': Google Employees Protest Work for the Pentagon," *New York Times*, April 4, 2018, https://www.nytimes.com/2018/04/04/technology/google-letter-ceo-pentagon-project.html.

17 OpenAI, "OpenAI's Approach to AI and National Security," October 24, 2024, https://www.openai.com/global-affairs/openais-approach-to-ai-and-national-security/.

18 David Vergun, "DOD Makes Loans to Industry for Critical Technology Development, Production," *U.S. Department of Defense News*, November 7, 2024, https://www.defense.gov/News/News-Stories/Article/Article/3960199/dod-makes-loans-to-industry-for-critical-technology-development-production/.

19 Jim Mitre and Joel B. Predd, *Artificial General Intelligence's Five Hard National Security Problems* (Santa Monica, CA: RAND Corporation, February 2025), https://www.rand.org/content/dam/rand/pubs/perspectives/PEA3600/PEA3691-4/RAND_PEA3691-4.pdf.

20 Haley Britzky, "Hegseth Announces He's Ending Pentagon Involvement in Trump Initiative Empowering Women Championed by Ivanka Trump and Rubio," *CNN*, April 29, 2025, https://www.cnn.com/2025/04/29/politics/hegseth-ending-pentagon-trump-women-initiative/index.html.

21 Amy Webb, T*he Big Nine: How the Tech Titans and Their Thinking Machines Could Warp Humanit*y (New York: PublicAffairs, 2019), https://www.hachettebookgroup.com/titles/amy-webb/the-big-nine/9781541773745/?lens=publicaffairs.

22 U.S. Congress, Senate, Committee on Armed Services: Emerging Technologies and Their Impact on National Security, 117th Cong., 1st sess., 2021, 117-148.

23 Defense Innovation Unit, "The Replicator Initiative," Defense Innovation Unit (DIU), https://www.diu.mil/replicator.

24 Ibid.

25 Albert A. Nofi, "Defining and Measuring Shared Situational Awareness," CNA, November 2000, https://www.cna.org/reports/2000/D0002895.A1.pdf.

26 IBM, "What Are AI Hallucinations?," *IBM Think*, September 1, 2023, https://www.ibm.com/think/topics/ai-hallucinations.

27 Katherine Chandler, "Does Military AI Have Gender? Understanding Bias and Promoting Ethical Approaches in Military Applications of AI," UNIDIR, December 7, 2021, https://www.unidir.org/publication/does-military-ai-have-gender-understanding-bias-and-promoting-ethical-approaches.

28 Cade Metz and Karen Weise, "A.I. Is Getting More Powerful, but Its Hallucinations Are Getting Worse," *New York Times*, May 5, 2025, https://www.nytimes.com/2025/05/05/technology/ai-hallucinations-chatgpt-google.html.

29 Ericka Johnson and Saghi Hajisharif, "The Intersectional Hallucinations of Synthetic Data," *AI & Society 40* (2025): 1575–1577, https://doi.org/10.1007/s00146-024-02017-8.

30 Ian M. Shaughnessey, "The Ethics of Robots in War," NCO Journal, February 2, 2024, https://www.armyupress.army.mil/Journals/NCO-Journal/Archives/2024/February/The-Ethics-of-Robots-in-War/.

31 Jimena Sofía Viveros Álvarez, "The Risks and Inefficacies of AI Systems in Military Targeting Support," Humanitarian Law & Policy Blog (International Committee of the Red Cross), September 4, 2024, http://blogs.icrc.org/law-and-policy/2024/09/04/the-risks-and-inefficacies-of-ai-systems-in-military-targeting-support/.

32 Azmat Khan, "Hidden Pentagon Records Reveal Patterns Of Failure In Deadly Airstrikes," *New York Times*, December 18, 2021, https://www.nytimes.com/interactive/2021/12/18/us/airstrikes-pentagon-records-civilian-deaths.html.

33 Lucy Suchman, "Briefing Paper: CCW Informal Meeting of Experts on Lethal Autonomous Weapons, Geneva, 12 April 2016, Panel 'Towards a Working Definition of LAWS': Autonomy," April 12, 2016, https://eprints.lancs.ac.uk/id/eprint/86141/1/CCW_Autonomy_Suchman.pdf.

34 Chandler, "Does Military AI Have Gender? Understanding Bias and Promoting Ethical Approaches in Military Applications of AI."

35 The Campaign to Stop Killer Robots, accessed February 20, 2025, https://www.stopkillerrobots.org/.

36 Ray Acheson, *A WILPF Guide to Killer Robots*, Women's International League for Peace and Freedom (Geneva), January 2020, https://www.wilpf.org/wp-content/uploads/2020/04/WILPF_Killer-Robots-Guide_EN-Web.pdf.

37 Vera Bergengruen, "How Tech Giants Turned Ukraine Into an AI War Lab," *Time*, February 8, 2024, https://time.com/6691662/ai-ukraine-war-palantir/; Paul Mozur and Adam Satariano, "A.I. Begins Ushering In an Age of Killer Robots," *New York Times*, July 2, 2024, https://www.nytimes.com/2024/07/02/technology/ukraine-war-ai-weapons.html.

38 Yuval Abraham, "'Lavender': The AI Machine Directing Israel's Bombing Spree in Gaza," *+972 Magazine*, April 3, 2024, https://www.972mag.com/lavender-ai-israeli-army-gaza/; Michael Biesecker, Sam Mednick, Garance Burke, and Abby Sewell, "As Israel Uses U.S.-Made AI Models in War, Concerns Arise About Tech's Role in Who Lives and Who Dies," *Associated Press*, February 28, 2025, https://www.ap.org/news-highlights/best-of-the-week/first-winner/2025/as-israel-uses-u-s-made-ai-models-in-war-concerns-arise-about-techs-role-in-who-lives-and-who-dies/.

39 Congress.gov, "S.3247 - 115th Congress (2017-2018): Women's Entrepreneurship and Economic Empowerment Act of 2018," January 9, 2019, https://www.congress.gov/bill/115th-congress/senate-bill/3247.

40 U.S. Department of Defense, "DOD Directive 3000.09, Autonomy in Weapons Systems," January 25, 2023, https://media.defense.gov/2023/Jan/25/2003149928/-1/-1/0/DOD-DIRECTIVE-3000.09-AUTONOMY-IN-WEAPON-SYSTEMS.PDF.

41 United Nations, "The Convention on Certain Conventional Weapons," accessed February 20, 2025, https://www.un.org/disarmament/the-convention-on-certain-conventional-weapons/.

42 United Nations General Assembly, Seventy-ninth session, "Lethal Autonomous Weapons Systems," A/C.1/79/L.77, October 18, 2024, https://documents.un.org/doc/undoc/ltd/ n24/305/45/pdf/n2430545.pdf.

43 United Nations, *Governing AI for Humanity: Final Report* (New York: United Nations, 2024), https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf.

44 Hudson et al., "The Heart of the Matter: The Security of Women, The Security of States."

45 Valerie M. Hudson, Donna Lee Bowen, and Perpetua Lynne Nielsen, *The First Political Order, How Sex Shapes Governance and National Security Worldwide* (New York: Columbia University Press, 2021), https://cup.columbia.edu/book/the-first-political-order/9780231194662.

46 OSCE Office for Democratic Institutions and Human Rights (ODIHR), "Gender and Early Warning Systems," November 17, 2009, https://www.osce.org/files/f/documents/1/a/40269.pdf.

47 UN Women, "FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women," February 10, 2025, https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women.

48 The Economist Intelligence Unit, *Measuring the Prevalence of Online Violence Against Women*, March 1, 2021, https://onlineviolencewomen.eiu.com/.

49 Kristine Baekgaard, *Technology-Facilitated Gender-Based Violence* (Washington, DC: Georgetown Institute for Women, Peace and Security, 2024), https://giwps.georgetown.edu/wp-content/uploads/2024/06/Technology-Facilitated-Gender-Based-Violence.pdf.

50 Diana Park and Kinsey Spears, *Women, Peace, and Cybersecurity* (Washington, DC: New Lines Institute for Strategy and Policy, June 2023), https://newlinesinstitute.org/wp-content/uploads/20230628-Dossier-WPS-Cyber-NLISAP-FINAL.pdf.

51 U.S. Department of State, "Gendered Disinformation: Tactics, Themes, and Trends by Foreign Malign Actors," March 27, 2023, https://2021-2025.state.gov/gendered-disinformation-tactics-themes-and-trends-by-foreign-malign-actors/.

52 U.S. Department of State, "Gendered Disinformation."

53 White House Task Force to Address Online Harassment and Abuse, *Final Report and Blueprint* (Washington, DC: The White House, May 2024), https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/05/White-House-Task-Force-to-Address-Online-Harassment-and-Abuse_FINAL.pdf.

54 Jeffrey Dastin, "Amazon scraps secret AI recruiting tool that showed bias against women," *Reuters*, October 10, 2018, https://www.reuters.com/article/us-amazon-com-jobs-automation-insight/amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK08G.

55 Khari Johnson, "MIT takes down 80 Million Tiny Images data set due to racist and offensive content," *Venture Beat*, July 1, 2020, https://venturebeat.com/ai/mit-takes-down-80-million-tiny-images-data-set-due-to-racist-and-offensive-content/.

56 Douglas Guilbeault et al., "Online Images Amplify Gender Bias," *Nature* 626, no. 8001 (February 14, 2024): 1049–1055, https://www.nature.com/articles/s41586-024-07068-x.

57 Karen Hao, "This is how AI bias really happens—and why it's so hard to fix," *MIT Technology Review*, February 4, 2019, https://www.technologyreview.com/2019/02/04/137602/this-is-how-ai-bias-really-happensand-why-its-so-hard-to-fix/.

58 Gaudys L. Sanclemente, "Digital Tools: Safeguarding National Security, Cybersecurity and AI Bias," *CEBRI Revista*, 2023, https://cebri.org/revista/en/artigo/112/digital-tools-safeguarding-national-security-cybersecurity-and-ai-bias.

59 Joy Buolamwini and Timnit Gebru, "How Well Do IBM, Microsoft, and Face++ AI Services Guess the Gender of a Face?," 2018, http://gendershades.org/.

60 National Academies, "Advances in Facial Recognition Technology Have Outpaced Laws, Regulations; New Report Recommends Federal Government Take Action on Privacy, Equity, and Civil Liberties Concerns," January 17, 2024, https://www.nationalacademies.org/news/2024/01/advances-in-facial-recognition-technology-have-outpaced-laws-regulations-new-report-recommends-federal-government-take-action-on-privacy-equity-and-civil-liberties-concerns#:~:text=Addressing%20specific%20use%20concerns%2C%20such,of%20political%20and%20civil%20liberties.

61 Sofia Gomez, "The Dangers of Militarizing Racist Facial Recognition Technology," *Georgetown Security Studies Review*, September 30, 2020, https://georgetownsecuritystudiesreview.org/2020/09/30/the-dangers-of-militarizing-racist-facial-recognition-technology/.

62 Amrita Kapur, Callum Watson and Anna-Lena Schluchter, "Policy Brief: Gender, Preventing Violent Extremism and Countering Terrorism Policy Brief Gender, Preventing Violent Extremism and Countering Terrorism," February 25, 2020, https://www.osce.org/files/f/documents/f/7/447094.pdf.

63 Nina Jankowicz, "The threat from deepfakes isn't hypothetical. Women feel it every day," *Washington Post*, March 25, 2021, https://www.washingtonpost.com/opinions/2021/03/25/threat-deepfakes-isnt-hypothetical-women-feel-it-every-day/.

64 Associated Press, "YouTube Creators Will Soon Have to Disclose Use of Generative AI in Videos or Risk Suspension," *AP News*, November 14, 2023, https://apnews.com/article/youtube-artitifical-intelligence-deep-fake-ai-creaters-0513fd9fddbd93af327f0411dd29ff3d.

65 Kyle Wiggers, "Deepfake detectors and datasets exhibit racial and gender bias, USC study shows," *Venture Beat*, May 6, 2021, https://venturebeat.com/ai/deepfake-detectors-and-datasets-exhibit-racial-and-gender-bias-usc-study-shows/.

66 Congress.gov, "S.146 - 119th Congress (2025-2026): TAKE IT DOWN Act," May 19, 2025, https://www.congress.gov/bill/119th-congress/senate-bill/146.

67 DoD Responsible AI Working Council, "U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway," DOD, June 2022, https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF.

68 Ibid.

69 Lisa Schirch, Report No.201: *Deliberative Technology: Designing AI and Computational Democracy for Peacebuilding in Highly-Polarized Contexts* (Tokyo: Toda Peace Institute, 2024), https://toda.org/policy-briefs-and-resources/policy-briefs/deliberative-technology-designing-ai-and-computational-democracy-for-peacebuilding.html.

70 The White House, "United States Government Women, Peace, and Security Congressional Report 2022," July 2022, https://oursecurefuture.org/sites/default/files/2025-02/2022-US-Women-Peace-Security-Congressional-Report.pdf.

71 Sanam Naraghi Anderlini, Women Building Peace: What They Do, Why It Matters (Boulder: Lynne Rienner, 2007), https://www.rienner.com/title/Women_Building_Peace_What_They_Do_Why_It_Matters.

72 UN Women, "Women's Participation And A Better Understanding Of The Political," 2015, https://wps.unwomen.org/participation/.

73 United Nations, Governing AI for Humanity: Final Report (New York: United Nations, 2024), https://www.un.org/sites/un2.un.org/files/governing_ai_for_humanity_final_report_en.pdf.

74 Congress.gov, "H.R.6216 - 116th Congress (2019-2020): National Artificial Intelligence Initiative Act of 2020," March 12, 2020, https://www.congress.gov/bill/116th-congress/house-bill/6216.

75 Congress.gov, "H.R.4346 - 117th Congress (2021-2022): CHIPS and Science Act," August 9, 2022, https://www.congress.gov/bill/117th-congress/house-bill/4346.

76 The White House, "Executive Order 14110, Safe, Secure, and Trustworthy Development and Use of AI," November 1, 2023.

77 The American Presidency Project, "Executive Order 14177 - President's Council of Advisors on Science and Technology," January 23, 2025, https://www.presidency.ucsb.edu/documents/executive-order-14177-presidents-council-advisors-science-and-technology.

78 The White House, "Executive Order on Promoting the Export of the American AI Technology Stack," July 23, 2025, https://www.whitehouse.gov/presidential-actions/2025/07/promoting-the-export-of-the-american-ai-technology-stack/.

79 The White House, "Executive Order on Modernizing Defense Acquisitions and Spurring Innovation in the Defense Industrial Base," April 9, 2025, https://www.whitehouse.gov/presidential-actions/2025/04/modernizing-defense-acquisitions-and-spurring-innovation-in-the-defense-industrial-base/.

80 National Institute of Standards and Technology, "AI Risk Management Framework," January 2023, https://www.nist.gov/itl/ai-risk-management-framework.

81 U.S. Department of Defense, "DoD Digital Modernization Paper: DoD Information Resource Management Strategic Plan FY19-23," July 12, 2019, https://media.defense.gov/2019/Jul/12/2002156622/-1/-1/1/DOD-DIGITAL-MODERNIZATION-STRATEGY-2019.PDF.

82 U.S. Department of Defense, "DOD Adopts Ethical Principles for Artificial Intelligence," February 24, 2020, https://www.defense.gov/News/Releases/Release/Article/2091996/dod-adopts-ethical-principles-for-artificial-intelligence/.

83 U.S. Department of Defense, "Executive Summary: DoD Data Strategy: Unleashing Data to Advance the National Defense Strategy," September 30, 2020, https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF.

84 Deputy Secretary of Defense, "Memorandum For Senior Pentagon Leadership Commanders Of The Combatant Commands Defense Agency And Dod Field Activity Directors," U.S. Department of Defense, May 26, 2021, https://media.defense.gov/2021/May/27/2002730593/-1/-1/0/IMPLEMENTING-RESPONSIBLE-ARTIFICIAL-INTELLIGENCE-IN-THE-DEPARTMENT-OF-DEFENSE.PDF.

85 U.S. Department of Defense Responsible AI Working Council, "U.S. Department Of Defense Responsible Artificial Intelligence Strategy And Implementation Pathway," June 2022, https://media.defense.gov/2022/Jun/22/2003022604/-1/-1/0/Department-of-Defense-Responsible-Artificial-Intelligence-Strategy-and-Implementation-Pathway.PDF.

86 U.S. Department of Defense Responsible AI Working Council, "U.S. Department of Defense Responsible Artificial Intelligence Strategy and Implementation Pathway."

87 CDAO, "Chief Digital and Artificial Intelligence Office," accessed February 20, 2025, https://www.ai.mil/.

88 U.S. Department of State, Bureau of Cyberspace and Digital Policy, accessed February 20, 2025, https://www.state.gov/bureaus-offices/deputy-secretary-of-state/bureau-of-cyberspace-and-digital-policy/.

89 U.S. Department of State, "Political Declaration on the Responsible Military Use of Artificial Intelligence and Autonomy," accessed October 2025, https://www.state.gov/bureau-of-arms-control-deterrence-and-stability/political-declaration-on-responsible-military-use-of-artificial-intelligence-and-autonomy.

90 U.S. Department of State, "Enterprise Data and Artificial Intelligence Strategy," September 2025, https://www.state.gov/wp-content/uploads/2025/09/Department-of-State-Enterprise-Data-and-AI-Strategy.pdf.

91 United States Agency for International Development (USAID), Digital Strategy 2020–2024 (Washington, DC: USAID, 2020), PDF, via ECHOcommunity, https://www.echocommunity.org/en/resources/04ea3fba-9298-4668-84fe-c0ee4119fc7e.

OUR SECURE FUTURE

WASHINGTON, DC, USA
OURSECUREFUTURE.ORG
@OURSECUREFUTURE

Women make the difference.