DCAF/CRC POLICY BRIEF

DCAF Geneva Centre for Security Sector Governance

Canadian Red Cross / Croix-Rouge canadienne

GENDER AND WPS IN MILITARY AI: IMPLICATIONS FOR IHL COMPLIANCE



ADVANCING WOMEN, PEACE, AND SECURITY AND GENDER PERSPECTIVES IN INTERNATIONAL HUMANITARIAN LAW: MOVING FROM ANALYSIS TO IMPLEMENTATION

KARYN STONE AND MEGAN BASTICK

AUGUST 2026

SUMMARY

Artificial intelligence (AI) is increasingly integrated into military decision-making systems, including intelligence analysis, targeting, and operational planning. While AI technologies may have operational advantages, they also introduce new risks for compliance with international humanitarian law (IHL), particularly in relation to the requirements of distinction, proportionality, precautions, and the assurance of accountability for violations.

States currently hold different views about the extent to which existing IHL obligations sufficiently regulate AI-enabled military systems. While states continue to debate whether new legally binding rules on autonomous weapons systems (AWS) are necessary, there is broad agreement that IHL applies to the use of AI-enabled military systems as it does to all weapons, means, and methods of warfare.

This policy brief proposes that gender analysis and the Women, Peace, and Security (WPS) framework are not peripheral considerations but are operationally relevant tools for supporting IHL compliance in the development and use of AI-enabled military systems and throughout the AI life cycle. When properly integrated, they can also strengthen civilian harm mitigation by improving situational awareness and reducing bias.



© Norwegian Armed Forces / Henriette Harkestad Alvheim / Rzeszów-Jasionka, Poland / Air Defense in Rzeszów / 2025

Based on discussions at an expert roundtable convened in March 2026 by DCAF and the CRC with military actors, legal experts, gender experts, and technical specialists, this brief identifies six overarching recommendations for states.

1. Treat gender bias and data limitations as legal risks in AI-enabled operations.
2. Establish gender-responsive governance of AI-enabled military systems.
3. Use AI to strengthen gender-responsive civilian harm mitigation.
4. Embed gender considerations into legal reviews of new weapons, means, or methods of warfare.
5. Embed gender considerations into the procurement of AI-enabled systems.
6. Strengthen women's meaningful participation and the use of gender expertise in AI governance.

This policy brief is part of a series published in DCAF's project 'Advancing WPS and Gender Perspectives in IHL: Moving from Analysis to Implementation'. This project is supported by the Government of the Principality of Liechtenstein.



© UN Photo / Albert Gonzalez Farran / A member of the Chinese Formed Police Unit deployed with UNMIL operates a drone with a video camera / 2018

CONTEXT

AI systems are increasingly integrated into military workflows, including intelligence processing, risk assessments, targeting, and civilian harm assessment. These systems rely on datasets and modelling that may reflect and amplify existing social biases. These biases can affect proportionality assessments, the identification of military objectives, and the effectiveness of precautionary measures, with direct implications for compliance with IHL. Gender analysis and the WPS framework offer opportunities to identify and potentially mitigate these risks.

This policy brief uses the term 'AI-enabled military systems' to encompass all military capabilities that incorporate AI technologies. This includes systems that support surveillance, operational planning, targeting, or civilian harm mitigation as well as AWS.

This brief is intended for military legal advisers (LEGADs), defence and military policymakers, operational planners, procurement and capability authorities, and stakeholders concerned with the governance, development, acquisition, and operational use of AI-enabled military systems.

The issues addressed in this brief are particularly relevant for military lawyers and policymakers, because decisions affecting compliance with IHL occur long before AI-enabled systems are operational and military operations take place. As AI-enabled systems become more integrated into military decision-making, LEGADs are increasingly required to advise not only on individual strikes or operations, but also on the broader systems, governance structures, and processes. In this context, LEGADs are uniquely positioned to help translate WPS commitments and gender analysis into legally relevant safeguards and oversight mechanisms across the AI life cycle.

The responsible use of AI-enabled military systems requires multidisciplinary engagement across all military and defence functions, including commanders, intelligence staff, procurement authorities, Gender Advisers, and training organizations.

CORE IHL PRINCIPLES

International humanitarian law (IHL) is a body of international law that seeks to limit the effects of armed conflict by protecting people who are not or are no longer participating in hostilities. IHL also restricts the means and methods of war. Any use of AI-enabled systems must comply with existing IHL provisions, namely:

Distinction

Parties to conflict must distinguish, at all times, between civilians and combatants and between civilian objects and military objectives.

Proportionality

Attacks are prohibited if the incidental damage is excessive in relation to the direct military advantage anticipated.

Precautions in attack

Parties to conflict must take all feasible precautions in the planning and execution of attacks to avoid or minimize incidental civilian harm.

These principles apply to all weapons, means, and methods of warfare, including AI-enabled technologies.

IHL AND AI

As has been affirmed at the United Nations General Assembly, IHL applies to all material uses of AI-enabled systems in both international and non-international armed conflicts, including where they are used in the conduct of hostilities.[1] The use of AI-enabled systems must comply with existing rules that regulate the conduct of hostilities, including those relating to distinction, proportionality, and precautions in attack.

The use of AI-enabled systems to support military functions, including surveillance, logistics, and decision-making, does not remove or displace legal accountability under IHL. AI-enabled systems that qualify as new weapons, means, or methods of warfare must also be subject to new weapons legal review.

A number of legal and operational questions concerning IHL and AI are subject to ongoing debate and discussion, particularly in international forums. This includes the Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems (GGE LAWS), the Global Commission on Responsible Artificial Intelligence in the Military Domain (REAIM), and the UN General Assembly First Committee.

One concern is the notion of *human judgement and control,* including 'context-appropriate human judgement and control', 'effective human judgement and control', and 'meaningful human judgement and control'. While humans must retain responsibility for implementation of IHL, states, legal experts, and international organizations continue to discuss what constitutes sufficient human involvement in AI-enabled military decision-making. High-paced operational settings may make meaningful human judgement more difficult. Systems must therefore be designed and governed to ensure effective human judgment and control is possible. For the purpose of this brief, context-appropriate, effective, or meaningful human judgement and control are commonly understood in line with the ICRC's definition as 'the type and degree of control that preserves human agency and upholds moral responsibility in decisions to use force'.[2]

The degree of permissible autonomy within military systems, including under what, if any, conditions AI-enabled systems select or engage targets without human intervention, raises important legal and operational questions. These include questions about accountability for decision-making and the ability to address violations of IHL if decisions are taken by AI-enabled systems. AI systems used in military operations are often procured from private sector actors that design, develop, and maintain them. Their involvement introduces additional complexity regarding accountability, oversight, and the allocation of responsibility between state and private actors.

AI systems have limitations regarding transparency, data quality, and bias, which can affect the reliability of outputs. Gender bias, discussed below, is especially relevant because it can distort assessments of civilian populations and civilian harm. These factors affect the reliability of outputs used in operational decision-making and have implications for legal compliance. The challenge is not whether IHL applies to AI-enabled military systems, but whether these limitations affect the ability to comply with existing legal obligations. It is in this space that WPS and gender considerations become increasingly relevant, as they directly impact how protection, including civilian harm mitigation, is understood in AI-enabled military systems.

APPLYING IHL WITH A GENDER AND WPS LENS

IHL contains rules aimed at limiting the impacts of armed conflict. Applying a gender perspective in this context means recognizing that conflict settings, impacts on civilians, and patterns of harm are not gender neutral. Women, men, girls, and boys experience the effects of armed conflict in different ways due to societal roles and expectations, differential access to resources, caregiving responsibilities, and pre-existing structural inequalities. These experiences are also shaped by intersecting factors such as age, ethnicity, socioeconomic status, and disability. As such, the application of IHL should consider these different experiences to ensure its protections are implemented without discrimination.

Failing to account in a context-specific manner for gendered patterns of life in intelligence gathering and analysis can lead to overlooking indicators of civilian life or civilian vulnerabilities. Likewise, the reverberating effects of attacks, such as displacement and loss of healthcare and social services, which are part of foreseeable incidental civilian harm, often affect women and girls disproportionately. Thus failure to integrate a gender perspective into information collection, interpretation, and operationalization and IHL decision-making processes can contribute to targeting errors, such as inaccurate distinction decisions, incomplete proportionality assessments, and inadequate precautions.

Gendered dynamics of civilian harm are further discussed in the DCAF/CIVIC Policy Brief 'Improving Civilian Protection by Incorporating Gender into Civilian Harm Mitigation Tools and Processes'.

The WPS Agenda provides an important framework for addressing gendered risks and patterns of harm in armed conflict. WPS and IHL can be mutually reinforcing: IHL sets legal requirements for conduct in conflict, while WPS provides practical guidance and offers institutional mechanisms (such as gender analysis, gender training, and Gender Advisers) to translate those requirements into military planning, operations, and decision making. The WPS Agenda complements IHL protections by mandating, for example, gender-responsive early warning and protection measures, prevention of conflict-related sexual and gender-based violence, mechanisms to ensure women's voices and participation, and gender mainstreaming in all aspects of peace and security.

A gender perspective is relevant across the full spectrum of IHL implementation. It can strengthen compliance with obligations relating to the conduct of hostilities, detention, access to healthcare, humanitarian relief operations, and the protection of civilians by helping decision-makers understand how different groups experience conflict and access protection.

Gender analysis – the systematic gathering and examination of information on the roles, inequalities, and needs of men, women, boys, and girls – can support more effective implementation of IHL obligations through better data and understanding to inform operational planning and implementation. Gender analysis and gender perspectives can be seen as vital to meeting IHL's non-discrimination requirements by helping decision makers identify how rules apply in practice across different populations.

For a more general reference on integrating a gender perspective into defence institutions, see the DCAF, OSCE/ODIHR, UN Women Tool, 'Defence and Gender'.

RECOMMENDATIONS

These six recommendations provide practical measures for states to strengthen compliance with IHL in the context of AI-enabled military systems. They underscore that gender analysis and the WPS framework are directly relevant to IHL implementation. These measures are intended to support activities across the full life cycle of AI systems, from design and procurement through operations and post-operations review.

RECOMMENDATION 1: TREAT GENDER BIAS AND DATA LIMITATIONS AS LEGAL RISKS IN AI-ENABLED OPERATIONS

Gender bias and data limitations in AI-enabled military systems must be understood not only as technical challenges but as a potential source of legal risk that may affect compliance with IHL.

AI targeting support systems may, for example, reproduce assumptions that military-aged men are more likely to be lawful targets without adequately accounting for context. They may fail to account for women's and men's different civilian patterns of life and vulnerability, or fail to recognize the different impacts of an attack on men, women, boys, and girls. This could result in incomplete assessments of who is present in an area, the likely effects of an attack on different civilian populations, or the precautions necessary to minimize civilian harm. It could also result in the miscategorization of a target as a military objective. Gaps in sex – and age-disaggregated data can further limit the ability of AI-enabled systems to account for gendered impacts in operational environments. Military personnel may themselves hold biases, including about how men and women behave or are vulnerable in conflict, that AI systems could amplify.

Where bias affects the accuracy or interpretation of AI-generated outputs, or where data reflecting the differences and inequalities between men, women, boys, and girls is missing from system design and training, this undermines IHL decision-making related to distinction, proportionality, or precautions necessary to minimize civilian harm in attacks.

Operationally, particular attention should be paid to risks of automation bias (the human tendency to overtrust and excessively depend on AI and automated decision-support systems) and lack of meaningful human judgement and control, especially in high-pressure operational environments. These can contribute to gender and other information biases passing unnoticed.

Ideally, states should conduct bias risk assessments throughout the full AI life cycle, including design, development, testing, training, and review (AI procurement is discussed in recommendation 5). Military AI systems often rely on commercial datasets and algorithms that are not fully transparent as to their assumptions and limitations for the states purchasing the systems, making it difficult for users to identify or correct bias. In some cases they are not even fully transparent to the system developers.

Gendered data, gender analysis, and other context-specific data should inform AI-enabled systems where operationally relevant. Sex – and age-disaggregated data can inform, for example, evacuation means, routes, and planning around civilian objects such as

hospitals and schools. Gender considerations (including failures to collect disaggregated data) should be integrated into training related to AI decision-support systems to increase understanding of these inherent limitations.

States should strengthen training for commanders, decision-makers, and AI operators to allow them to assess AI-enabled outputs critically in operational environments. They must understand system limitations – gendered and otherwise – in terms of data biases and missing data, and, where possible, counter automation bias. Militaries should involve Gender Advisers in analysis and planning processes concerned with using AI tools, and ensure LEGADs are trained in gendered impacts to inform legal analysis. At the same time, a commander or operator of an AI tool often will not be able to address biases inherent in the system's design or training adequately. In high-tempo environments it will often not be realistic or operationally feasible for commanders or operators to detect and correct, for example, failures within the AI system itself to account for differentiated civilian impacts. These risks must be continuously considered and mitigated upstream.

In many cases it will not be possible to mitigate gender bias in the datasets feeding AI systems. When bias cannot be properly mitigated and can contribute to the risk of IHL violations, the use of AI-enabled systems should be limited. Furthermore, states should support international dialogue on appropriate limits to the use of AI-enabled weapons systems where bias cannot be effectively mitigated.



© Pexels / Matthew Hintz / 2021

RECOMMENDATION 2: ESTABLISH GENDER-RESPONSIVE GOVERNANCE OF AI-ENABLED MILITARY SYSTEMS

When AI-enabled military systems lack transparency and, for example, rely on opaque datasets or unclear decision-making processes, it may be difficult to assess compliance with IHL obligations, evaluate gender bias, or attribute responsibility for decisions and actions. Governance mechanisms for military AI should ensure meaningful oversight throughout the AI life cycle to address these potential gaps in accountability. Oversight mechanisms should not be limited to internal military reviews, but should include parliamentary committees, government watchdogs, and independent auditors.

Particular care should be taken concerning the risk of dual use of AI systems, when systems designed for military purposes are also used for civilian purposes.

More holistically, states should ensure that AI-enabled military systems are governed by frameworks that ensure both compliance with IHL obligations and meeting commitments under the WPS Agenda. This includes embedding gender-responsive safeguards and IHL safeguards across the entire military AI life cycle, from policy and doctrine to procurement and design, deployment and review, and oversight. Specifically, effective governance requires mechanisms that can identify and address risks in a proactive manner, not only at the point of use or through corrective action after harm occurs.

Existing civilian AI governance frameworks may be useful models for militaries to adapt. States should consider how AI risk and impact tools could be applied or adapted to military contexts, including frameworks such as the Fundamental Rights and Algorithm Impact Assessment developed by the Netherlands.[3]

States should establish clear legal and policy expectations regarding data transparency, gender perspectives, and accountability, as well as creating accountability mechanisms and after-action review processes.

Gender-related legal commitments, policies, or contractual requirements should not be treated as stand-alone mechanisms for mainstreaming gender in AI governance. They should be rooted in a broader ecosystem of experts working on gender, security, and technology. This integration can support the breaking down of silos between communities working on similar agendas but within different policy processes or domains. For example, a growing body of expertise and practice exists on gender in cyber security, including the implications of data, bias, and technology-related harms.[4] It is important to ensure that AI governance is expressly connected to these types of existing expertise and frameworks.

WPS National Action Plans (NAPs) can provide an entry point for states to connect gender equality commitments with emerging technologies. For example, Kenya's NAP on WPS recognizes the importance of integrating WPS principles into AI strategies, alongside strengthening gender-sensitive digital legislation. This approach demonstrates how WPS frameworks can serve as a mechanism for linking gender considerations with broader technology governance agendas.[5]

RECOMMENDATION 3: USE AI TO STRENGTHEN GENDER-RESPONSIVE CIVILIAN HARM MITIGATION

As AI is increasingly embedded in military operations, without safeguards, there is a risk that gendered patterns of movement and life are overlooked, resulting in incomplete assessments and weakened civilian protection outcomes. Gender analysis should be incorporated into operational decision-making, including targeting processes, civilian harm mitigation measures, and operational review mechanisms. This requires embedding gender considerations, not as an add-on but as a core component of data collection, interpretation, and operationalization across AI-enabled systems.

Civilian harm assessments and after-action review processes should analyse differentiated impacts across populations to strengthen institutional learning, accountability, and future civilian protection measures for all users of AI-enabled military systems.

Operations should integrate context-specific and sex – and age-disaggregated data, particularly in assessments related to detention, civilian movements, and evacuation planning. Feedback loops between operational outcomes and system refinement processes should be strengthened to ensure that these lessons inform future development and operational decisions for AI-enabled military systems. Furthermore, commanders, analysts, and operators should be trained to assess AI-enabled outputs accurately and account for differentiated civilian impacts in operational decision-making.

States can proactively strengthen civilian harm mitigation practices through gender analysis and the use of disaggregated data and context specific analysis. AI-enabled systems may help identify patterns of civilian movement, needs or vulnerabilities if they are designed and deployed in a way that protects against discriminatory outcomes.

During the expert roundtable, the DELTA AI system in use in Ukraine was shared as an example of how information on civilian movements could be used to support humanitarian aid planning, including by distinguishing between different population groups, such as adults and children. AI systems may also help in identifying barriers to humanitarian access and whether aid reaches different groups affected by conflict. Throughout the life cycle, these systems must be subject to oversight mechanisms to ensure data protection, non-discrimination principles, and a do-no-harm approach.

RECOMMENDATION 4: EMBED GENDER CONSIDERATIONS INTO LEGAL REVIEWS OF NEW WEAPONS, MEANS, OR METHODS OF WARFARE

Legal reviews of new weapons, means, or methods of warfare, including those with AIenabled capabilities, should examine how bias in data or modelling assumptions may affect compliance with IHL. Legal reviews stem from Article 36 of Additional Protocol I to the Geneva Conventions,[6] which requires states parties to determine in the study, development, acquisition, and adoption of a new weapon, means, or methods of warfare whether its employment would, in some or all circumstances, be prohibited under international law.

Building on good practice from Article 36 review processes,[7] legal review mechanisms should explicitly assess whether applicable AIenabled systems may reproduce or amplify genderrelated bias in ways that affect IHL compliance. To support these assessments,

states should ensure that those conducting the reviews have access to relevant expertise, including in gender analysis, data governance, AI systems, and bias mitigation. If expertise does not exist within existing review structures, states should develop appropriate institutional capacity through training or engagement with relevant experts.

Reviews should examine how datasets, modelling assumptions, and system limitations may impact distinction, proportionality, precautionary measures, and non-discrimination in operations. Legal reviews should extend beyond assessing system and technical performance to consider how AI-enabled systems may affect protected and vulnerable populations in practice. This reflects emerging interpretations of Article 36 emphasizing that gender is integral to assessing the foreseeable humanitarian effects of weapons systems, means, and methods, and ensuring compliance with applicable IHL obligations and protections against adverse distinction.[8]

Reviews should include assessment of data representativeness and resulting bias, as well as whether systems can account for gendered civilian behaviour in relevant operational contexts. There must be an evaluation of whether risks arising from the use of limited datasets can be adequately mitigated to ensure compliance. Reviews should examine system design, considering the level of human judgement and control and availability of verification prompts or delays in high-risk contexts. Reviews should also consider how operators will account for gendered patterns of life or other factors that influence how women, men, girls, and boys are impacted by conflict, and how this information is used to assess the lawfulness of a weapon and its use.

These considerations align with various state positions in the GGE LAWS' discussions on AWS and broader responsible AI governance standards. States can also draw on good practice under the Arms Trade Treaty, where gender-sensitive risk analysis is integrated into arms transfer assessments, including the potential for weapons to exacerbate gender-based violence and other differentiated civilian harms.[9]

However, this recommendation cannot be implemented without a foundational Article 36 review mechanism that is already in place. For those states that lack established Article 36 review processes or the technical or gender expertise to undertake them, capacity-strengthening measures such as training and multidisciplinary cooperation will be required to support implementation. International exchanges of good practices may also contribute to effective integration of gender considerations into Article 36 reviews.

Where risks of gender bias and legal non-compliance cannot be sufficiently mitigated through technical, procedural, or operational safeguards, Article 36 reviews should identify conditions, restrictions, or prohibitions on use. In line with good practice on weapons life-cycle governance, findings from legal reviews should inform procurement decisions, governance development, training, and equipment transfer procedures, ensuring a coherent approach to limiting harm across the full life cycle of AI-enabled weapons and weapons systems.

RECOMMENDATION 5: EMBED GENDER CONSIDERATIONS INTO PROCUREMENT OF AI SYSTEMS

As the private sector contributes significantly to the development, production, and use of AI in military contexts, military procurement is a key process through which states implement legal obligations and policy commitments on responsible AI, shaping design and operational outcomes. Many existing procurement approaches remain underdeveloped in the systematic integration of IHL compliance and gender-responsive safeguards.[10] States should integrate IHL compliance, gender-responsive safeguards, bias mitigation, and risk management across the military AI procurement life cycle, including supplier selection, contractual requirements, testing, auditing, and monitoring.

Procurement contracts should include enforceable obligations relating to transparency, monitoring, reporting of incidents or failures, and continuous testing to prevent additional risks such as bias and discriminatory impacts. This is particularly important in situations where systems are acquired from foreign vendors relying on models that limit access to training data, system logic, or performance information. States should include clear enforcement provisions, including suspension or termination clauses when suppliers fail to meet contractual requirements. These contractual measures should complement, rather than replace, state obligations to ensure AI-enabled military systems can be used in compliance with IHL.

Financial and procurement measures can be leveraged to incentivize responsible development by establishing expectations for AI-enabled military systems before they are acquired. States can require suppliers to demonstrate prior to purchase how they have identified risks related to IHL compliance, gender bias, and dataset limitations, and incorporate gender-responsive safeguards through system development. This can include evaluation criteria that assess transparency of datasets and methodologies, bias mitigation, and monitoring how systems work across different contexts and populations.

Existing instruments regulating private security services outsourced by states, including the Montreux Document[11] and the International Code of Conduct for Private Security Service Providers,[12] can support this. The DCAF Contract Guidance Tool is one such aid for private military and security services that operationalizes international legal obligations through procurement. The tool translates normative standards into binding contractual clauses, requirements, and monitoring mechanisms.[13]

Engagement with industry is necessary to ensure that operational and legal requirements are incorporated during the military AI development, acquisition, and life-cycle management process. This should include informed dialogue on legal requirements, data transparency, system design, bias, and oversight.

States should, moreover, establish regular dialogue between defence procurement personnel, LEGADs, technical experts, industry, and WPS networks working on disarmament issues to inform procurement standards for AI-enabled military systems. WPS and gender expertise could help ensure that procurement frameworks integrate gender-responsive safeguards and are aligned with WPS commitments. Multistakeholder engagement is needed to break down silos and promote cross-learning.

Finally, states should invest in incentivizing AI for civilian protection measures, including tools that could identify early warning indicators of conflict-related sexual violence, and those that support more effective humanitarian response planning. This would include gender-sensitive analysis of civilian harm and needs assessments in conflict environments.

RECOMMENDATION 6: STRENGTHEN WOMEN'S MEANINGFUL PARTICIPATION AND THE USE OF GENDER EXPERTISE IN AI GOVERNANCE

Women account for only 22–30 per cent of the global AI workforce and hold under 14 per cent of senior executive roles in AI development and governance. Numerical underrepresentation in these roles constrains the range of professional experiences, technical backgrounds, and analytical perspectives that inform critical decisions in system design. When women are largely absent from technical and leadership positions, structural vulnerabilities, including inadequate consideration of gender-differentiated impacts, are more likely to remain unidentified during development, testing, and deployment phases.[14] States should support the full, equal, and meaningful participation and influence of women across all stages of the development, acquisition, use, and governance of AI-enabled military systems. This encompasses women's participation in policy development, procurement, legal reviews, and evaluation, and in leadership, technical, legal, and operational roles.

States should ensure that gender analysis is integrated into AI-enabled military systems at every stage of the life cycle. This requires deliberate incorporation of gender expertise (specialized knowledge and skill in analysing how gender roles, dynamics, and inequalities affect societies, laws, and policies) into policy development, procurement decisions, legal review, technical evaluation, and operational assessment. Gender expertise may be held by women or men, constituting a distinct professional capability separate from, although complementary to, women's participation in development and governance roles.

States should, moreover, recognize their gaps in gender expertise within the private, technical, and military sectors, including lack of expertise on how to operationalize gender-responsive approaches. They should invest in institutional gender capacity, both drawing experienced gender experts into AI processes as advisers and implementing education and training to ensure that all key stakeholders, technical and military, have adequate understanding of gender bias and its manifestations in military systems. Gender expertise should not be treated as a standalone policy commitment but as part of the multidisciplinary expertise needed to develop and use AI-enabled military systems responsibly.

States should engage with women-led and civil society organizations in the development and implementation of weapons governance mechanisms. Their expertise and connection to a diversity of community voices can support the identification of unforeseen risks of AI-enabled military systems. Civil society engagement has proven effective in similar governance settings, including around the Arms Trade Treaty and the Anti-Personnel Mine Ban Convention. Civil society has provided independent analysis on humanitarian impacts, and incorporated perspectives from women, girls, and communities and evidence of the importance of gender-responsive approaches.

Finally, states should promote engagement with diverse professionals, including in civil society, academia, technology companies, and other technical fields, who can inform understandings of how social assumptions and inequality can be embedded in AI system design. Such engagement across industry can support more transparent assessments of risks, ultimately strengthening transparency, accountability, and civilian protection outcomes.

CONCLUSION

AI-enabled military systems are reshaping how decisions are informed and made in armed conflict, but they do not alter the applicability of IHL or diminish the responsibilities of parties to conflict to ensure compliance. The growing involvement of private sector actors in the development and maintenance of AI-enabled military systems does not diminish state obligations under IHL. Ensuring IHL compliance requires deliberate gender-responsive governance choices that reinforce human judgement, address bias, and integrate gender analysis to ensure an accurate understanding of civilian harm and maintain accountability.

The recommendations in this brief demonstrate that gender-responsive approaches should be integrated across the full AI life cycle, from governance and procurement to legal review, operational use, civilian harm mitigation, and institutional capacity. Gender analysis and the WPS framework strengthen the implementation of existing IHL obligations by improving understanding of civilian populations, reducing bias, and supporting informed decision-making.



© UN Photo / Evan Schneide / Informal consultations on Lethal Autonomous Weapons Systems / 2025

This brief also underscores that technical safeguards are not the only necessary mitigation measure to address the risks associated with AI-enabled military systems. States should build institutional capacity by integrating gender expertise and multidisciplinary oversight into existing structures. This means ensuring that commanders, planners, intelligence personnel, procurement authorities, LEGADS, and Gender Advisers are equipped to apply gender analysis throughout the AI-enabled systems life cycle, which will further reinforce compliance with IHL.

The recommendations in this brief highlight that governance responsibilities begin long before systems are deployed. Procurement policies, Article 36 review processes, planning, and governance development, including the meaningful participation of both women and gender experts, all support ensuring that AI-enabled military systems can be used in compliance with IHL. States should implement proactive governance approaches, embedding legal compliance and civilian protection considerations upstream in system design, rather than relying solely on commanders and operators to mitigate AI-enabled outcomes that rely on incomplete information during military operations.

Some states may require capacity building and international cooperation to support implementation.

Finally, the brief recognizes that some uses of AI may pose risks that cannot be properly mitigated, requiring restrictions, conditions limiting use, or prohibitions to ensure compliance with IHL. Such approaches are currently being discussed by numerous military and security institutions. As military AI capabilities continue to grow, states should strengthen international dialogue by sharing good practices, developing effective governance, and enhancing discussions on legal and operational limits, including the circumstances in which restrictions, limitations on use, or prohibitions may be necessary to ensure compliance with IHL. Integrating gender perspectives and WPS considerations into these discussions can help ensure good policies and practices, while recognizing that some uses of AI may never be compatible with IHL.

NOTES

1 United Nations General Assembly, *Artificial intelligence in the military domain and its implications for international peace and security*, A/RES/80/58.

2 International Committee of the Red Cross (ICRC), *Ethics and Autonomous Weapon Systems: An Ethical Basis for Human Control?*, Geneva, 2018.

3 Ministry of the Interior and Kingdom Relations, *Impact Assessment Fundamental Rights and Algorithms*, Government of the Netherlands, 2021.

4 Julia-Silvana Hofstetter and Panthea Pourmalek, *Gendering Cybersecurity through Women, Peace and Security: Gender and Human Rights in National-Level Approaches to Cybersecurity*, Global Network of Women Peacebuilders and ICT4Peace Foundation, 2023.

5 Republic of Kenya, *Kenya National Action Plan on Women, Peace and Security 2025–2029*, Nairobi, 2025.

6 *Protocol Additional to the Geneva Conventions of 12 August 1949, Relating to the Protection of Victims of International Armed Conflicts* (Protocol I), 8 June 1977, art. 36.

7 ICRC, *A Guide to the Legal Review of New Weapons, Means and Methods of Warfare: Measures to Implement Article 36 of Additional Protocol I of 1977*, Geneva, 2006.

8 Tess Bridgeman and Lauren Kahn, 'Gendering the Legal Review of New Means and Methods of Warfare', *Just Security*, 2022.

9 Small Arms Survey, *At Whose Risk? Understanding States Parties' Implementation of Arms Trade Treaty Gender-based Violence Provisions*, Geneva, 2022.

10 Netta Goussac and Vincent Boulanin, *Responsible Procurement of Military Artificial Intelligence*, Stockholm International Peace Research Institute, 2026.

11 ICRC and Swiss Confederation, *The Montreux Document on Pertinent International Legal Obligations and Good Practices for States Related to Operations of Private Military and Security Companies During Armed Conflict*, Montreux Document Forum, 2008.

12 International Code of Conduct Association, *The International Code of Conduct for Private Security Service Providers*, 2010.

13 DCAF, *A Contract Guidance Tool for Private Military and Security Services*, Geneva, 2017.

14 Ana Carmo, 'AI is getting women wrong as gender bias persists, data reveals', UN Women, New York, 2026; Jelena Cupać, 'The gender code: Gendering the global governance of artificial intelligence', in *Handbook on the Global Governance of Artificial Intelligence*, Edward Elgar Publishing, 2026.

ACRONYMS AND ABBREVIATIONS

AI	Artificial Intelligence
AWS	Autonomous Weapons Systems
CRC	Canadian Red Cross
CHM	Civilian Harm Mitigation
DCAF	Geneva Centre for Security Sector Governance
GGE LAWS	Group of Governmental Experts on Emerging Technologies in the Area of Lethal Autonomous Weapons Systems
IHL	International Humanitarian Law
IHRL	International Human Rights Law
LEGAD	Legal Adviser
WPS	Women, Peace, and Security

RESOURCES

- The AutoPractices Project, 'Strengthening Human Agency in the Military Domain: Best Practices Toolkit for Policymakers, Developers, and Users of AI Systems', Center for War Studies, University of Southern Denmark, Odense, 2026
- Laura Bruun and Marta Bo, Bias in Military Artificial Intelligence and Compliance with International Humanitarian Law, Stockholm International Peace Research Institute, 2025
- Katherine Chandler, Does Military AI Have Gender? Understanding Bias and Promoting Ethical Approaches in Military Applications of AI, UNIDIR, Geneva, 2021
- DCAF, OSCE/ODIHR, UN Women, 'Defence and Gender' in *Gender and Security Toolkit*, Geneva, 2019
- Andrea Farrés Jiménez, 'Gendering the Legal Review of New Means and Methods of Warfare', Just Security, 2022
- Netta Goussac and Vincent Boulanin, 'Responsible Procurement of Military Artificial Intelligence', Stockholm International Peace Research Institute, 2026
- Shimona Mohan and Dongyoun Cho, 'Gender and Lethal Autonomous Weapons Systems', UNDIR, Geneva, 2024
- Lauren Spink and Vanja Kovac, 'Improving Civilian Protection by Incorporating Gender into Civilian Harm Mitigation Tools and Processes', DCAF and CIVIC, 2026
- UN Women, 'Action Brief – From Warfare to Peace building: Employing Artificial Intelligence for Women, Peace and Security | Publications | UN Women – Asia-Pacific', New York, 2022

AUTHORS

Karyn Stone, Canadian Red Cross and Megan Bastick, DCAF – Geneva Centre for Security Sector Governance

ACKNOWLEDGEMENTS

DCAF and the authors are grateful to colleagues, members of the IHL Community of Practice for WPS, and other reviewers for contributing to this policy brief. In particular, the authors thank Catherine Gribbin of the Canadian Red Cross; Line Barabant, Will Bennett, Anna Marie Burdzy, Nathalie Gendre, Zeineb Mansour, Rebecca Mikova, Gabrielle Priklopilova and Marlène Wäfler of DCAF; Sophie Aumailley, Laura Moorghen, Lieutenant Colonel Dirk Naessens, and Colonel Erik Op de Beeck of the Belgian Ministry of Defence; Captain Ahmed Chehaibi of the Tunisian Ministry of National Defense; and Alexandra Duca and Lauren Esquilant of the Austrian Federal Ministry of Defence.

DCAF Geneva Centre for Security Sector Governance

DCAF – Geneva Centre for Security Sector Governance is dedicated to improving the security of states and their people within a framework of democratic governance, the rule of law, respect for human rights, and gender equality. Since its founding in 2000, DCAF has contributed to making peace and development more sustainable by assisting partner states, and international actors supporting these states, to improve the governance of their security sector through inclusive and participatory reforms. It creates innovative knowledge products, promotes norms and good practices, provides legal and policy advice, and supports capacity-building of both state and non-state security sector stakeholders.

Canadian Red Cross Croix-Rouge canadienne

As a member of the Red Cross and Red Crescent Movement, the **Canadian Red Cross**'s mission is to help people and communities in Canada and around the world in times of need and support them in strengthening their resilience. In particular, the CRC's IHL unit aims to protect the dignity and lives of people affected by armed conflict by supporting IHL in Canada and around the world through education, training, advocacy, and humanitarian diplomacy.

ISBN Number 978-92-9222-833-0

© DCAF and Canadian Red Cross, 2026. Use, translation, and dissemination of this publication are encouraged. We do, however, ask that you acknowledge and cite materials and do not alter the content.

Design: Nadia Joubert

Cover photo: © Pexels / Shalom de León / 2020

DCAF Geneva Centre for Security Sector Governance

Maison de la Paix
Chemin Eugène-Rigot 2E
1202 Geneva, Switzerland

+41 (0) 22 730 94 00
info@dcaf.ch
www.dcaf.ch

Canadian Red Cross
Croix-Rouge canadienne