Filling the Blanks: Putting Gender into Military A.I.

Shimona Mohan

Abstract
Defence structures around the world are seeing a technological upheaving as new and emerging technologies like artificial intelligence (AI) are being added to military arsenals. However, military AI largely lacks precision and is often developed without any threat-modelling which takes gender into account, examples of which are already being seen in civilian applications of AI. Translated into a conflict environment, deploying such AI systems could mean that women and other genders would be disproportionately impacted by algorithmic biases. As military AI becomes more commonplace, the imperative is to mobilise gender-equal agendas for security and emerging technologies. This brief examines the gender-shaped gaps in the application of military AI and offers multi-faceted solutions to fill them.
Assuring gender-equal futures is a common and constant mantra for many industries and activities around the world, even though backlash against women's rights seems to be underway in the recent past. Progress on the gender front, when it is tangible, appears in staccatos; sustained, tangible, meaningful changes have been hard to incorporate into pre-existing or even developing structures and processes. According to the United Nations' Gender Snapshot 2022, the world is currently not on-track to achieve gender equality by 2030 as envisaged by the Sustainable Development Goals (SDGs). The report also cautioned that without increased investment and activity, the global community could take 300 years to realise gender equality.

Two very relevant themes are threaded throughout the UN report: those of the inextricable relations of gender with conflict, and with technology. Conflict situations further increase the likelihood, frequency and intensity of gender inequality on a number of metrics, and women's underrepresented and disadvantageous position vis-à-vis emerging technologies further narrows their prospects to progress towards equality. With emerging technologies like artificial intelligence (AI) now seeping into conflict situations, and given women's vulnerability with respect to both developments, it is essential to look at the specific ways in which this combination may specifically harm women and minority genders, as well as how these harms can be prevented or remedied.

This brief takes a multifaceted approach to identifying the gaps and their potential resolutions around the issue of gendered considerations in military AI. It sets the stage by contextualising the gender-military-technology nexus, and then highlights the gender-shaped gaps in military AI. The brief analyses the technology driving military AI, legal reviews of AI-based weapons, and normative policy processes around gender, security and technologies like AI to catalogue the various points at which the lack of a specific gendered perspective may become a hindrance. It then suggests targeted approaches to fill the identified blanks and closes with proposed cross-cutting measures that should form the bedrock of any attempt at gender-equitable technological development.
Feminist international relations theorists often posit that there is a distinct link between gender and war, wherein the relation between attackers and victims is akin to the gendered dynamics of power between men and women. Due to the way that militaries and security architectures have conventionally evolved, women are notionally considered victims of conflict and conflict-related sexual violence, while men are seen as soldiers and, thus, perpetrators of this violence.

This perception has resulted in what can be referred to as ‘militarised masculinities,’ i.e. the idea that real men are soldiers and real soldiers are men. These militarised masculinities have in turn resulted in ‘masculinised militaries,’ i.e. military cultures that regurgitate and repeat the notion of ‘military equals male’ through their structures and processes up to an almost imperceptible level. In this culture, even if women join the military as equals of men, they have been ‘othered’ and considered anomalies or supposedly inferior.

Apart from being masculinised, militaries are also highly advanced in terms of technologies for security applications. Armed conflict is increasingly making use of emerging technologies like AI, as has been evidenced in recent clashes in Ukraine, Libya, and the Nagorno-Karabakh region. AI is a force multiplier for military operations, and a growing number of countries are expanding their repertoire of military AI to take advantage of this. Military applications of AI are not, however, unidimensional. They are now increasing in their scope, quantum and magnitude, for instance as weapons like lethal autonomous weapons systems (LAWS), swarm and storm drones, anomaly detection systems, cognitive radars, target identification systems, and many others.

While AI is a revolutionary technology, it comes with its own set of problems with regard to gender. Although it may appear to be so, AI is not neutral – it can internalise and then catastrophically enhance gender biases that societies possess, programme them into AI, and/or ignore them in outputs in the absence of sensitivities to those biases, to begin with. Adding to this overarching issue is the specific and marked dearth of women tech professionals in fields like STEM (science, technology, engineering and mathematics) and ICT (information and communication technology), which makes it difficult to mainstream gender-specific issues in tech. Gendered considerations also do not feature meaningfully in either the development or deployment of military AI, or the policy processes around it. These high-stakes technologies are thus fundamentally conceived in a ‘gender vacuum’.
While women and minority genders have been harmed and adversely affected by the exclusion and inherent biases against them within both security and tech spheres analysed separately, an amalgamation of the two fields in the form of military AI would and does expectedly further exacerbate these. Recent studies have shown that about 92 percent of software professionals are men, and while the gender ratio of armed forces around the world varies greatly across countries and military cultures, women remain a minuscule fraction of the forces in an overwhelming majority of countries, ranging from 0.3 percent to 20 percent according to one estimate. Since militaries and technological fields are clearly already male-centric spaces and military technologies are thus developed in almost exclusively male-dominated environments, the propensity of gender-biased AI systems emerging out of them is reasonably high.

Gender is seen as a ‘soft’ security issue in policy considerations as opposed to ‘hard’ security deliberations which are given more focus. The inclusion of gender in tech (whether in terms of female workforce participation or gendered considerations in the development of new and emerging technologies) is also characterised as an ethical concern rather than a core tech one. This characterisation of gender as an add-on essentially makes it a non-issue in security and tech agendas. If at all it is present, it is usually put down as a check box to performatively satisfy policy or compliance-related compulsions.

“AI can internalise and then catastrophically enhance gender biases that societies possess, programme them into AI, and/or ignore them in outputs.”
To prevent gender from becoming an afterthought in the development of military AI systems, it is important to identify where the gendered gaps lie throughout the life cycle of these systems. In doing so, it is also possible to point out and/or predict the exclusive harms that could emerge out of overlooking the incorporation of gender in emerging technologies, and ultimately determine how to fill these blanks to make sure that these harms do not emerge when military AI systems become more commonplace.

Technological

Gender biases in AI systems\textsuperscript{17} can be a result of either the data that has been used to train and develop the system, and/or the processing of that data by the algorithms used by underlying machine learning (ML) models, and/or even the human counterparts of the operation who make decisions at different checkpoints of the development and use of the AI system. While the former two are usually the direct causes, the latter forms the implicit catalyst that allows the bias to progress and appear at the output stage.

The first step in developing any AI system is to have huge amounts of organised data, or datasets, to train the system to identify certain values and act contextually on them. If the datasets collected or selected are incomplete or skewed towards or against a sub-group, they will produce results that marginalise those sub-groups or make them invisible in some way. Since datasets about humans condense people to data points, proportionally misrepresenting people of certain genders or leaving them out of the dataset altogether would result in gender-biased or gender-invisible datasets.\textsuperscript{18} However, representative and updated datasets are quite rare, and there are a number of reasons for persistent data gaps, including low prioritisation of this kind of data. UN Women estimates that only 13 percent of countries have a dedicated budget for collecting and analysing disaggregated gender statistics.\textsuperscript{19}

Yet, even if a dataset is precise and representative of the intended population, gender-biased ML algorithms applied to the data may still result in biased outputs. In most supervised ML models, training datasets are given labels by a human developer to enable the ML model to classify the information it already has.\textsuperscript{20} The model then characterises new information given to it based on this classification syntax, after which it generates an output. There are two possible modes of introduction of biases in this process: first, if the human developer has
their own biases which they either introduce into the system or retain due to ignorant oversight; and second, if biases are incorporated in the processing of the data within the ‘black box’ of the AI/ML system, which is not explainable to or understandable by human operators. The black box, as the name suggests, makes the learning process of the system opaque, and its algorithms can thus only be fixed once an output is generated and the human developer affirms that there was a problem with processing the input data.

If the processing of this algorithm is fraught with implicit biases, the algorithm will continue to apply its biased ‘knowledge’ to other datasets as well. For instance, consider images of nurses being repeatedly labelled as or correlated to a woman and a doctor to a man, despite either gender being able to perform either of these jobs, and the human annotator either affirms this gendered labelling or does not correct this at the development or testing stage. Such a situation could produce more unintentional gender-biased outputs, like Apple’s sexist credit card algorithm that was revealed to provide a significantly higher credit line to male clients despite similar or even worse credit histories as compared to their female clients, with no other plausible differentiating factor apart from gender.

Multiple studies have shown that data and algorithms are responsible for the introduction and amplification of gender and race biases in incumbent AI systems. A Stanford study of publicly available information on 133 biased AI systems, deployed across different economic sectors from 1988 to 2021, found that 44 percent exhibited gender bias, including 26 percent that showed both gender and racial biases. Similar results have been obtained by other research, notably the Gender Shades study by the MIT Media Lab which evaluated how accurate AI-based gender classification services and facial recognition (FR) software were, when demarcated by identification of gender and skin colour. Their analysis showed that while most softwares recognise white male faces quite accurately, they do not recognise darker female faces up to 34 percent of the time.

Since technologies like AI are dual purpose in the way they are designed and used, civilian AI-based technologies like FR can be seamlessly transferred into conflict environments. In such cases, biases can then be intentionally or inadvertently programmed into military AI systems. Intentional target-profiling using FR softwares could be used for the potential targeting of men and boys in conflict areas, since women are not generally considered to be combatants.
and men are usually presumed to be so, even if they are civilians. On the flip side of the same example, given that FR systems already struggle with correctly identifying women in civilian applications, inadvertent AI bias may lead to unprecedented harms, such as misidentifying civilian women as non-human objects and engaging with them in conflict settings as such.

**Legal**

Apart from gender-sized blanks in the development and deployment of military AI systems themselves, there are also noticeable gaps in weapons review processes and national and international policy instruments around gender and military AI. All countries are required to conduct legal reviews of new weapons that they are developing before these are used in armed conflicts as per international law. Countries that are party to the First Additional Protocol (AP 1) of the Geneva Conventions are further required to use Article 36 of the Protocol to conduct specific weapons reviews. Article 36, which obligates States to determine whether their weapon, means or method of warfare could be prohibited by international law for any reason, has been a constant presence in the context of the use of LAWS on battlefields.

The power to conduct these reviews resides exclusively with militaries or allied national research and development agencies, and there is no system of checks and balances to ensure that the developed weapons are indeed in accordance with international law. Since national weapons reviews are insular and highly contextual, there is also no clarity around their methods, metrics or mechanisms to judge new weapons technologies. States have also not been able to agree upon voluntary sharing of best practices with each other drawn from their national reviews of AI-based weapons.

**Normative**

The applicability of international law-oriented weapons reviews of LAWS is still being debated in forums like the Group of Governmental Experts (GGE) under the Convention on Certain Conventional Weapons (CCW), and there is thus no stipulated standardisation in international policy to review weapons using military AI. The CCW GGE, as the only intergovernmental policy process that could potentially regulate LAWS, has also struggled to include any meaningful mentions of gender in its outcome documents. Consensus on this has been hard to reach and maintain, with many countries asking to strike out mentions of
‘gender biases’ as potential outcomes of the use of LAWS during the meetings, and instead using the more politically neutral terminology of ‘social biases.’

Both phrases have occasionally made it into final reports of the GGE proceedings, but have regularly faced resistance. While the last substantial report of the GGE on LAWS from 2021 makes specific mention of datasets that can amplify gender or race bias, an advance report of the 2023 sessions has no mention of biases. The future work of the GGE is now dependent on the Meeting of High Contracting Parties to the CCW later this year, but the general deadlock at the GGE which has prevented it from generating a normative and operational framework for LAWS has been a discouraging factor.

In the meanwhile, offshoots of the LAWS regulation process have sporadically taken place, such as the adoption of the Belén Communiqué by the Latin America and the Caribbean countries in February 2023, but gender bias still remains a missing consideration from such frameworks. Zooming in further, about 70 countries have so far also come up with their own national strategies, agendas, governance frameworks or dedicated funding and institutional set-ups for AI, but very few of them encompass ethical considerations including issues of bias, and information around global military uses of AI remains elusive and sporadic.

“Studies have shown that data and algorithms are responsible for the introduction and amplification of gender and race biases in incumbent AI systems.”
It is clear that there are a number of gaps where gender should be incorporated to make sure that military AI is not developed as a gender-independent technology. It is also apparent that these blanks are not unilateral in nature due to any single factor, hence there must be simultaneous, concerted efforts on various fronts—technological, legal and normative—to resolve them.

**Technological**

Potential gender gaps in military AI systems should be rooted out from inception, i.e. from the designing and development stage of the systems. Since inaccurate, skewed, and misrepresentative data can give gender-biased results, it is important to ensure that the datasets that are to be used to train the systems are fair and representative of diverse populations. This is not an easy task, since contextual gender-balanced datasets are not readily available and would essentially need to be created or enhanced from a primary unit level. The low prioritisation of gender-disaggregated data needs to be countered to ensure that representative datasets are effectively gathered and utilised.

Data2X, a civil society organisation under the United Nations Foundation, suggests several methods to ensure that gender-specific data are generated, maintained and regularly updated. Some of these include investing across all parts of the data collection system (with a focus on public offices like national statistics offices), utilising big data gathered from gadgets and online activity, sex and gender disaggregation of existing international databases, and more methodological work to contextually identify and standardise measures to collect and interpret gendered data. The OECD provides a toolkit for countries to mainstream and implement gender equality through self-assessment for gender-disaggregated data, and the Global Partnership on AI (GPAI) also identifies disaggregating data by gender as one way to build more effective and accurate AI systems for the future.

Once the datasets are in order, ML systems need to be audited to make sure they are not introducing, learning and/or amplifying any gender biases. The first step to prevent this is to make sure that human developers, annotators, testers, and operators of the systems are well-trained and gender-sensitised, so that they do not introduce or retain their own biases while working with the systems. Next, since the black box prevents the human developer from looking into the algorithmic processing of the datasets and fix any issues, it is
essential to employ new technologies and methods like Explainable AI (XAI) and corresponding XAI toolkits like those released by Google, Microsoft and IBM to ensure that military AI developers can look into the AI’s black box and figure out gender bias issues with the aim of resolving them. A gendered threat modelling process should ideally follow to ensure that there are no blind spots that have been unintentionally left behind.

**Legal**

Only a few countries are known to conduct weapons reviews, and gender-sensitive weapons reviews which help prevent biases and targeting of people solely based on gender are yet to be a particular consideration for any country. However, gendering existing weapons reviews has been floated recently by civil society as a possible starting point. This idea recommends conducting Article 36 reviews as usual, and then additionally disaggregating the resulting data by gender to analyse the potential specific effects that new weapons technologies like military AI could have on certain genders. Additionally, it suggests including experts with a particular understanding of or training in gender and military dynamics such as gender advisers and focal points to be part of the legal review processes.

**Normative**

On the policy front, although the CCW GGE on LAWS is essentially gridlocked, countries continue to stress that it is an appropriate forum for discussing LAWS, and it has thus continued with its meetings in 2023. Despite waning discussions around the potential adverse effects of LAWS on certain population groups distinguished by race and gender, gender-friendly countries like Canada, the Philippines, Ireland, Panama and Costa Rica continue to be vocal about the issue throughout ongoing sessions. Concentrated work on gender and military AI by associated epistemic communities around this nexus, including organisations like the Campaign to Stop Killer Robots, Reaching Critical Will and the UN Institute for Disarmament Research (UNIDIR), ensure that the gender issue remains on the agenda in some capacity as countries continue to grapple with the formulation of an overarching regulation on LAWS.
Outside of the CCW proceedings, the institution of an overarching feminist foreign policy (FFP)\(^48\) can help populate the GGE and future processes around military AI with more gendered considerations. While only a handful of countries currently subscribe to an FFP, the trend is slowly gaining political currency with three countries—Spain, Libya and Germany—having joined the group in 2021. Apart from FFPs, a much larger number of countries (currently over 100) have national action plans (NAPs)\(^49\) for national-level implementation of the UN Security Council Resolution 1325 on the Women, Peace and Security (WPS) agenda.\(^30\) As the gender-military-tech nexus becomes clearer and activity around it picks up pace, countries could also start including gender- and technology-related actions, including military AI, in these binding national frameworks.

The first step to prevent ML from amplifying gender biases is to make sure that human developers, annotators, testers, and operators are well-trained and gender-sensitised.
It is clear that there are a number of blanks when it comes to gender considerations in military AI, but most of them have potential corresponding solutions as well. Apart from the specific recommendations for the identified challenges, it is also crucial to ensure that cross-cutting measures like interdisciplinary evaluations of issues and experts who understand the gender-military-technology nexus are involved to find solutions to this and other similar problems. Intersectional and culture-specific approaches around gender should also be adopted as per the application potential of the military AI in question, and gender-sensitivity trainings should be part of both technology as well as military activity. It would also be beneficial to ensure that there are no exclusionary processes around the gender-military-tech nexus—tech and security developments should not entail ‘manels’ with only or mostly men. Equally importantly, gender-specific developments around tech and security should also not exclusively engage women and minority genders.

Net positive change can only result from an equitable exchange of experiences and ideas, coupled with consistent and multifarious actions around the inclusion of gender in all major tech and military developments. In this regard, a multi-pronged approach towards putting gender in military AI would also double up as an opportunity to offer durable solutions and ensure that gendered considerations are institutionalised as a part of not only military AI developments, but also any future iterations of military technology.

Shimona Mohan is a Research Assistant at ORF’s Centre for Security, Strategy and Technology.
1 “In focus: 16 Days of Activism against Gender-Based Violence,” UN Women, November 18, 2022, https://www.unwomen.org/en/news-stories/in-focus/2022/11/in-focus-16-days-of-activism-against-gender-based-violence#:~:text=Led%252oby%2520civil%2520society%252C%2520the%2520theme%2520under%2520the%2520Days%2520%E2%80%9CUNiTE%E2%80%9D.


4 “Men make war; women live with the consequences. At least that is the way it is largely perceived,” International Committee of the Red Cross (ICRC), October 11, 2018, https://www.icrc.org/en/document/women-war


13 UN Women, *Progress on the Sustainable Development Goals: The Gender Snapshot 2022*


Endnotes


Endnotes


Images used in this paper are from Getty Images/Busà Photography.