2 // 2024

spotlight

BEYOND THE CODE

Unveiling Gender Dynamics in AI and Cybersecurity for International Security

Emerging technologies are transforming foreign and security policy as they challenge traditional understandings of power, influence and security. Developments in artificial intelligence (AI) and the increasing importance of cyberspace are some of the most prominent in this regard. Yet, not only are there repercussions for security when narrowly conceived as *state security*, but they also affect gender relations and human security more broadly. Gender as an analytical category allows us to shed light on the impact of emerging technologies on inequalities, power and violence.

AI detection security camera feed from Mobile World Congress 2022
© picture alliance / NurPhoto | Joan Cros

BY ANNA-KATHARINA FERL AND CLARA PERRAS

Gender is highly relevant to international cybersecurity and AI technologies but is often overlooked and under-analyzed. Technology, security and gender are mutually reinforcing – gender influences technological developments and security policies and gendered violence is replicated and amplified through them. This is why we argue that international cybersecurity and the use of AI technologies are in need of a critical gender perspective to reveal and counter those unequal power structures and forms of violence. Neglecting the gendered dimensions of emerging digital technologies hinders the development of security practices aligned with the needs and realities of those most affected.

A gender perspective allows us to highlight how challenges such as hacking (i.e. unauthorized access, theft, destruction, or manipulation of information), disinformation, or structurally inbuilt biases may affect the security of vulnerable groups. Widespread hacking of sensitive health data containing information about abortions can lead to significant risks for patients and health workers in contexts where reproductive health and rights are not recognized.[1] Disinformation campaigns frequently target women, individuals of diverse sexual orientations, gender identities, expressions, and characteristics (SOGIESC), as well as human rights activists, subjecting them disproportionately to hate speech and violence.[2][3] Existing gender and racial biases are deeply ingrained in data sets used for training AI applications. AI models thus perpetuate discrimination by reproducing and reinforcing biases, often with unpredictable consequences.[4]

The rapid and global evolution of cyberspace – the virtual environment where communication, interaction and the exchange of information between computers, devices, and people takes place – is prompting states to enhance traditional security measures. They focus on safeguarding critical infrastructure and boosting military capabilities for potential cyber operations. Artificial intelligence today is largely based on machine learning (ML) algorithms that are used to classify large sets of data and recognize patterns in text, speech or images.[5] These AI technologies are increasingly being integrated into the military domain and cybersecurity, be it for rather mundane

GENDER & INTERSECTIONALITY

Gender relates to social and cultural norms, behaviors, and identities that are assigned to specific gender categories. In most societies, gender is constructed within a male and female binary and determines who holds power and has access to resources.

Because gender is not the only power structure, an intersectional approach is needed that takes into consideration context specific forms of discrimination and oppression on ground of class, ethnicity, race, age, nationality, and more.[6]

activities such as logistics, improving and increasing military decision-making or enhancing autonomous functions in weapons systems.[7]

However, issues surrounding digital technologies and security have predominantly been discussed within supposedly gender-neutral but deeply male-centric and militarized paradigms and understandings of security. Additionally, the perception of threats and the development of protective measures have been shaped by a largely homogenous – white and male – group, inadvertently side-lining the unique experiences, expertise, and vulnerabilities of women and other marginalized groups. It is imperative to recognize gendered and intersecting power structures as a crucial variable influencing cyber-security and military AI applications.

UNDERSTANDING THE NEED OF GENDER ANALYSIS FOR DIGITAL TECHNOLOGIES

Existing international frameworks in the field of disarmament, as well as the United Nations Women, Peace, and Security (WPS) agenda, have become recognized frameworks for addressing gender as an issue for international security. More recently, feminist foreign policies are slowly beginning to engage with cybersecurity and emerging AI technologies. An intersectional feminist perspective on security first entails the deconstruction of mainstream security discourses and practices and then the analytical refocusing on diverse security needs and experiences of violence by marginalized groups. Violence can be understood as a continuum that includes, in addition to physical violence, other dimensions such as structural, economic, discursive, or cultural violence.[11] This is why a feminist approach is imperative to sustainably mitigate the layered risks amplified and reproduced in and through cyberspace and AI technologies for individuals, structurally disadvantaged groups, societies, and states.

But how exactly does gender shape security, AI technologies and cyberspace? Two aspects that determine the relation of gender and security have to be highlighted.[12] First, international security policy and our thinking about war and violence is embedded in gendered power structures that privilege masculine forms of knowledge and action, as well as state-centric and militarized security understandings. This becomes evident in the domination of male personnel in the field of international security, in their applied strategies and military thinking but also in masculine language.[13]

Second, not only is the physical world is shaped by gendered structures and violence, but these are reproduced in cyberspace and through AI as humans are developing and using the newly created spaces, tools and instruments.[14]

Gender therefore influences the definition and scope of security policies and gendered hierarchies and practices mutually reinforce each other. It is, like other fields relevant for international security, highly dominated by masculine and militarized thinking that translates into corresponding action. Applying an intersectional gender lens to cyberspace and military AI in the context of international security means to acknowledge a wide range of insecurities that otherwise remain invisible. Those become evident in (1) unequal participation and representation, (2) reinforced gender biases through AI and (3) issues of data protection and privacy.

UNEQUAL PARTICIPATION AND REPRESENTATION

The underrepresentation and lower participation of marginalized groups has been a constant feature of security politics, not only when it comes to cybersecurity and AI. However in these areas, these tendencies become glaringly obvious.

In all aspects of the cybersecurity profession, women and people with diverse SOGIESC are underrepresented. Only 24% of the cybersecurity workforce worldwide are women;[15] of these, 9% Black, 4% Hispanic and 8% Asian women make up only a very small proportion of the total workforce. Although global statistics show[16] that the number of women is increasing, more than half of all women in cybersecurity feel like they can't reach higher positions in their organizations; an experience that is much higher for women that are also part of a minority. The same trends can be observed in the field of AI professions. While the number of women in computer science and AI has been increasing, only around 22% of AI computer scientists are women.[17] Even more troubling is the glo-

UNDERREPRESENTATION

In arms control, non-proliferation and disarmament fora heads of delegations are mostly men and women only account for 20%-32% of delegates in multilateral meetings.[8] In cyber diplomacy, women only made up on average 20% of participants within the UN Groups of Governmental Experts (GGE). Only 24% of delegations were led by women.[9] During the first UN expert meeting on autonomous weapons systems in 2014, of the 18 experts who were invited, none were women.[10]

OGBV

OGBV can be understood as part of the continuum of violence against women and people of diverse SOGIESC as violence offline and online are mutually reinforcing each other. In traditional understandings of cybersecurity, forms of OGBV are largely neglected. It describes "a range of different forms of violence perpetrated by ICT means on the grounds of gender or a combination of gender and other factors.[18] The most common forms are cyber stalking, cyber harassment, cyber bullying, online gender-based hate speech and non-consensual intimate image abuse. It becomes visible in the context of intimate partner violence[19] but also in gendered disinformation campaigns and hate speech.[20]

bal inequality of representation among support workers labelling datasets for training, who are overwhelmingly located in the Global South.[21]

Reasons for the lack of equal participation and representation are plentiful. Unequal access to education, individual priorities, masculine work culture in the digital sector, unequal distribution of care work and the influence of norms that associate technical skills with men. The fields of natural science, technology, engineering and mathematics (STEM) are traditionally male dominated which means that gendered norms and assumptions as well as patriarchal structures are reproduced. While representation can only be a first step in overcoming gender inequalities and won't solve underlying structural issues, it is nonetheless important to integrate meaningful perspectives and experiences of marginalized groups.[22]

AI REINFORCES GENDER BIASES

A recent study on publicly available instances of biases in AI machine learning systems found that 44.2% of those systems demonstrate gender bias and 25.7% both gender and racial bias.[23] But where do these biases come from and what do they mean? Through these biases, outputs were incorrect and/or discriminatory. These biases arise because machine learning algorithms reproduce or even amplify social gender norms. First, programmers might reproduce unintentional biases because, as pointed out above, AI work and computer science lack diversity and equal representation. Second, the data itself can exhibit gendered and racialized stereotypes that are then reproduced through the algorithms when social groups are over- or underrepresented or misclassified.[24] The consequences of gender biases being reinforced by technologies are even more serious in military AI applications.[25] In targeting decisions for instance, the distinction between combatants and civilians is essential. If however, autonomous or AI-supported targeting decisions are influenced by gender biases, ‚military-aged men' will most likely be disproportionately miscategorized as combatants and thus as potential targets. AI and other digital technologies are also increasingly integrated into cybersecurity systems and responses, resulting in biased threat models[26] or reporting with severe gender blind-spots. On the other hand, AI also creates new gendered risks in the realm of cybersecurity. Deep fakes are manipulated videos that can be indistinguishable from originals and are becoming more and more accessible and realistic due to increased quality and availability of tools. Gendered security concerns arise as deep fakes can lead to image-based sexual violence, impacting victims personally and professionally with women being disproportionally affected.[27]

GENDERED RISKS OF DATA PROTECTION AND PRIVACY

Data protection and privacy rights are already discussed politically and represent an established part of cybersecurity talk. What current discussions are still missing are specific gendered risks that arise as a result from the fact that not all people are equally affected by invasions of their privacy. Privacy International traces back how the right to privacy has historically been (and still is) interpreted for the exercise of patriarchal power, for example, by legitimizing domestic violence, including rape.[28] This leads to the double threat for the rights of women and people of diverse SOGIESC, because they are violated both in the public sphere and in the private sphere, the latter of which is supposed to guarantee protection from state intervention. These restrictions and threats are significantly expanded by digital technologies. Groups facing structural discrimination, activists, human rights defenders and journalists are especially affected by state surveillance and excessive data collection, as impressive research shows.[29] In Iran, Lebanon and Egypt, people with diverse SOGIESC do not only face surveillance but are also under threat of physical violence as fake accounts in dating apps are being used "to lure individuals into face-to face-meetings, entrap them, and subject them to arrest or cruel and degrading treatment, or blackmail them for money or sexual services".[30]

Also, data breaches have gendered impacts as data collection is never gender neutral. The digital collection of health data and breaches of that data, which can include information on pregnancies or abortions, can lead to the legal and social discrimination and stigmatization of women and people with diverse SOGIESC, thus to the violation of their sexual and reproductive rights. In the US, the 2022 reversal of Roe v. Wade—which granted the constitutional right to abortion in the US—is an example of how gendered cybersecurity risks can emerge and worsen.[31]

THE AUTHORS

Anna-Katharina Ferl is doctoral researcher at PRIF's research department "International Security" and member of the research group "Emerging Disruptive Technologies". Clara Perras is a researcher at PRIF's "Glocal Junctions" research department.

CONTACT

ferl@prif.org, perras@prif.org

PRIF, Baseler Str. 27–31, 60329 Frankfurt am Main
PVst, DPAG 43853, Entgelt bezahlt, ISSN-2512-627X

WHAT CAN WE DO ABOUT IT?

As illustrated above, cybersecurity and AI technologies are multilayered and impact more than state security. Yet, international security is still largely characterized by state and military-centric security and structural violence. A feminist perspective on cybersecurity and emerging technologies like AI challenges conventional concepts and provides an opportunity to examine the diverse dimensions and contexts in which security policies unfold and unravel existing power structures. Becoming aware of how gender shapes cybersecurity and AI and acknowledging and centering gendered risks as well as traditional security is a first step in the right direction towards a security approach that takes seriously the realities of marginalized groups and tackles root causes of violence. However, all too often these perspectives remain siloed. National cyber- and AI security strategies need to be gender-mainstreamed.[32] Next steps for policy makers include the development of gender sensitive policies, cybersecurity and AI standards on all levels and in private and public sectors. Already existing frameworks like WPS and feminist foreign policies need to address questions of cybersecurity and emerging AI technologies more explicitly to remain credible. The involvement of relevant stakeholders in decision-making processes international fora and national security policies, especially those traditionally marginalized, is essential. Other steps should include increasing the participation of women and other marginalized groups in STEM and in security policy fora, as well as incorporating alternative security approaches and mechanisms, developed from and with affected communities. With the accelerated speed in which technological innovation in the field of AI and cyberspace takes place, regulatory policies are needed more than ever - and these have to include an intersectional gender perspective to ensure that gender-based threats will not be overlooked, societal resilience against cyberattacks strengthened, and resources more fairly distributed.

PRIF SPOTLIGHT: The Peace Research Institute Frankfurt (PRIF) is the largest institute for peace research in Germany. PRIF sets out to analyze the causes of violent international and internal conflicts, carrying out research into the conditions necessary for peace and working to spread the concept of peace.

V.i.S.d.P.: Lion Tsarfin, Press and Public Relations (PRIF), Baseler Straße 27–31, 60329 Frankfurt am Main, Phone (069) 959104-0, info@prif.org, www.prif.org. Design: Anja Feix · Layout: PRIF · Print: Druckerei Spiegler

Peace Research Institute Frankfurt
Leibniz-Institut für Friedens- und Konfliktforschung

Leibniz Association

References and further reading:
prif.org/spotlight0224-fn
DOI 10.48809/prifspot2402