


Gendering Cybersecurity through Women, Peace and Security: Gender and Human Rights in National-level Approaches to Cybersecurity



Authors: Julia-Silvana Hofstetter, ICT4Peace Foundation
Panthea Pourmalek, Global Network of Women
Peacebuilders (GNWP)

Editor: Mavic Cabrera-Balleza, GNWP

Project Advisors: Anne-Marie Buzatu, ICT4P, Katrina Leclerc, GNWP

Acknowledgments

This report was prepared by the Global Network of Women Peacebuilders (GNWP) and ICT4Peace Foundation, with support from the Swiss Federal Department of Foreign Affairs, Directorate of International Law (DIL).

The authors are grateful to interviewees for their time and support and would like to thank: Veridiana Alimonti (EFF), Fitri Bintang Timur (CSIS), Alexi Drew (RAND Europe), Myriam Dunn Cavelty (CSS, ETH Zurich), Merle Maigre (e-Governance Academy), Elizabeth Mendoza (Hiper Derecho), Allison Pytlak (WILPF), Marija Ristic (Brinn Network), Julia Słupska (University of Oxford), James Shires (University of Leiden), Sarah Shoker (Open AI).

Disclaimer:

The Report Brief is the independent work of GNWP and ICT4Peace. The views expressed in this report do not necessarily reflect those of the project's supporters or of anyone who provided input to, or commented on, drafts.

© Global Network of Women Peacebuilders and ICT4Peace Foundation 2023

This research is published under the Creative Commons Attribution 4.0 International License. You may use and adapt the material included herewith, provided that you give appropriate credit to the Global Network of Women Peacebuilders, ICT4Peace Foundation, and the authors, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the Global Network of Women Peacebuilders or ICT4Peace Foundation endorse you or your use.

Suggested citation: Hofstetter, J.-S., & Pourmalek, P. (2023). Gendering Cybersecurity through Women, Peace and Security: Designing Conflict-Sensitive Strategy Documents at the National Level. Global Network of Women Peacebuilders and ICT4Peace Foundation. <http://gnwp.org/gender-cybersecurity-through-women-peace-security>

Table of Contents

1. INTRODUCTION.....	6
1.1 Overview and summary.....	6
1.2 Methodological note	7
2. CONCEPTUAL NOTES ON CYBERSECURITY AND GENDER	8
2.1 Adopting a Human-Centric Approach to Cybersecurity	8
2.2 Gender and cybersecurity.....	10
2.3 Intersectionality and what we mean with 'women' and 'gender'	13
2.4 Conflict-sensitive cybersecurity and 'do no harm'.....	14
3. OVERVIEW OF KEY POLICIES AND DISCUSSIONS AT NATIONAL AND INTERNATIONAL LEVELS	15
3.1 Gender and cybersecurity at the multilateral level.....	15
3.1.1 Multilateral Cybersecurity Fora.....	15
3.1.2 Multilateral gender and human rights documents.....	16
3.2 Gender and cybersecurity at the national level.....	18
3.2.1 Gender in National Cybersecurity Policies.....	18
3.2.2 Cybersecurity in WPS NAPs.....	19
3.3 How the WPS framework can be used to re-design cybersecurity policies.....	20
4. GENDER AND CYBERSECURITY IN NATIONAL POLICIES: SYNERGIES BETWEEN NCSS AND WPS NAPs.....	21
4.1 Gender-sensitivity in national cybersecurity policies.....	21
4.1.1 Gender Mainstreaming National Cybersecurity Policies.....	22
4.1.2 Inclusive Multi-stakeholder Engagement	23
4.1.3 Opportunities and Limitations of NCS as vehicles for gender-sensitive cybersecurity.....	24
4.2 Integration of cybersecurity into the NAPs on WPS.....	25
4.2.1 Cybersecurity in the development NAPs on WPS.....	25
4.2.2 Toward more cyber-sensitive NAPs.....	25
4.2.3 Good practices from the NAP development process.....	26
4.2.4 Limitations of NAPs as vehicles for gender-sensitive cybersecurity.....	27
5. CYBERSECURITY IN CONFLICT-AFFECTED CONTEXTS	28
5.1 Cyber vulnerabilities unique to fragile settings.....	28
5.2 The impact of cyber threats on peacebuilding.....	28
6. RECOMMENDATIONS.....	29

ABBREVIATIONS

CEDAW – Convention on the Elimination of Discrimination Against Women

CSO – Civil Society Organization

GBV – Gender-Based Violence

GGE – Group of Governmental Experts

ICT – Information and Communication Technology

ITU – International Telecommunications Union

NAP – National Action Plan

NCS – National Cybersecurity Strategy

OEWG – Open-Ended Working Group

UN – United Nations

UN HRC – United Nations Human Rights Council

UNSC – United Nations Security Council

WPS – Women, Peace and Security

1. INTRODUCTION

1.1 Overview and Summary

In remarks made on 23 May 2022, Under-Secretary-General Rosemary DiCarlo emphasized the “significant new risks” of technological advances. The Under-Secretary-General recognized the progress made by Member States in “establishing a normative framework to ensure responsible behavior in cyberspace,” primarily through the UN General Assembly. She further called for building consensus on the use and risks of digital technologies, alongside other Our Common Agenda components, including the New Agenda for Peace.

A Case for Gender-Sensitive Cybersecurity

This report explores the new risks posed by emerging and modern technologies through a gender lens, in particular, that of the Women, Peace and Security agenda. The benefits of approaching cybersecurity from a gender perspective are threefold. First, it allows for an acknowledgment that women and other marginalized groups in society experience and use the cyberspace differently. They are often disproportionately harmed by cyber threats or faced with particular gendered cyber harms. The gendered nature of cybersecurity extends beyond cyber threats and into drafting and implementation of cybersecurity policy. International and national cybersecurity policies often neglect women’s and other vulnerable groups’ particular needs resulting from the gendered cyber threat landscape. These groups’ representation in cybersecurity policymaking and technology development is limited, increasing the risk of perpetuating gender inequality through cybersecurity policies and the general digitalization of public service. A clear understanding of the complexities of women’s experiences in cyberspace due to structural inequalities, combined with accountability and political commitment, may result in more effective cybersecurity policies. Second, it creates the potential to improve women and other marginalized groups’ access to cybersecurity provisions, from emergency response to legal remedies, which are often limited due to pre-existing discriminatory societal structures. These groups are also more often affected by unintended negative consequences of state actions in cyberspace. Third, incorporating a gendered perspective helps to address blind spots in cybersecurity policy. Adopting a human-centric and gender-sensitive approach to cybersecurity is crucial to fill gaps in cybersecurity policies created by the state- and business-centric approaches. Such approaches create a limited view of cyber threat assessments and options for cybersecurity provision and stand as a barrier to more holistic and effective cybersecurity responses.

Growing Interest in Gender Perspectives in National and International Cybersecurity

There is a growing awareness on the multilateral level of the need to integrate a gender perspective into international cybersecurity. Along these lines, state, and civil society actors have called for this purpose to apply the Women, Peace, and Security agenda (WPS), along with international frameworks and conventions on gender equality, to these policies. However, less attention has been given to the implications of the WPS and other international frameworks for formulating policies. This study addresses this gap by analyzing the integration or non-integration of gender and women's rights in National Cyber Security Strategies (NCS) and how cybersecurity concerns are reflected or not reflected in National Action Plans (NAPs) on WPS and other relevant women's rights and gender equality policy instruments. Employing a WPS lens, it further explores a need for conflict-sensitive approaches to cybersecurity and the risks faced by conflict-affected populations, women and girls in conflict-affected and insecure contexts, and women and youth peacebuilders.

Recommendations

Based on the analysis conducted, the report recommends the following to improve the gender sensitivity of national-level approaches to cybersecurity:

1. Expand the definition of cybersecurity to include a human-centric approach, emphasizing human rights;
2. Raise the profile of gender issues by including a pledge to mainstream gender in all cybersecurity design and implementation processes;
3. Strengthen civil society's role through inclusive multi-stakeholder engagement; and
4. Subject each cybersecurity measure to a context-specific 'do no harm' assessment to ensure conflict-sensitive cybersecurity policies.

Detailed recommendations on capacity-building, awareness-raising, and building expertise in cybersecurity are available in section 6 of this report.

1.2 Methodological Note

GNWP and ICT4Peace Foundation conducted in-depth qualitative research to inform this report, including semi-structured key informant interviews (KIIs) and a review of relevant policies and frameworks. The research draws on 36 in-depth interviews with women peacebuilders, including those involved in the drafting of NAPs on WPS, digital activists, and cybersecurity and ICT experts. Interviews were conducted with participants from 24 countries, including Armenia, Brazil, Cameroon, Canada, Chad, Colombia, the Democratic Republic of the Congo (DRC), Georgia, Indonesia, Kenya, Lebanon, Nepal, Nigeria, Northern Ireland, Peru, the Philippines, Rwanda, Syria, Ukraine, Uganda, the UK, United States, Uruguay, and Yemen.

To complement the KIIs, GNWP and ICT4Peace Foundation organized three online consultations on "Gendering Cybersecurity through Women, Peace, and Security" in July and August 2022. The consultations focused on three regions: East and West Africa, Eastern Europe and the South Caucasus, and Latin America. The consultations brought

together women peacebuilders, women leaders, digital activists, and cybersecurity experts from Argentina, Armenia, Azerbaijan, Bolivia, Cameroon, Chad, Chile, Colombia, Costa Rica, DRC, Georgia, Kenya, Mali, Mexico, Nigeria, South Sudan, Tanzania, Uganda, Ukraine, Uruguay, and Zimbabwe. GNWP and ICT4Peace used the highlights of the regional consultations to verify the findings of this research report and to produce three regional advocacy strategies.

2. CONCEPTUAL NOTES ON CYBERSECURITY AND GENDER

2.1 Adopting a Human-Centric Approach to Cybersecurity

Cybersecurity can be loosely defined as “the set of protocols, technologies, and practices designed to protect against threats mediated by digital technologies.”¹ It is important to note that there is no singular or commonly agreed-upon definition of cybersecurity. Two dimensions of defining cybersecurity can be particularly contentious. First is the level of application of cybersecurity. Some definitions of cybersecurity focus on the state or interstate level, while others claim that cybersecurity has applications at other levels – such as the community or individual.² Second is the subject of cybersecurity. There exists debate around whether, beyond the protection of systems and infrastructure, cybersecurity should target the protection of information, spaces, or humans.³

Both levels carry implications for the inclusivity of cybersecurity. For example, many conceptions of cybersecurity at the state level focus primarily on protecting systems and critical infrastructure.⁴ This critical infrastructure, however, is mainly technical and considers only what is deemed essential for the continued operation of the state rather than what is vital for humans and ordinary citizens.⁵ Further, individuals and civil society can both be the target of cyber attacks and contribute to identifying cyber threats.⁶ Since the data collection and reporting of threats are mostly carried out by private and commercial actors, civil society and individuals are systemically excluded from common conceptual and operational definitions of cybersecurity.⁷

Addressing issues at the intersection of cybersecurity and gender require both societal and technical mitigation strategies”.⁸ Thus, conceptions of cybersecurity that



¹ Slupska, J. (2019). Safe at Home: Towards a Feminist Critique of Cybersecurity. *St. Anthony's International Review*, 15(1), 83–100. Available at SSRN: <https://ssrn.com/abstract=3429851>, 84.

² Millar, K., Shires, J., & Tropina, T. (2021). *Gender Approaches to Cybersecurity: Design, Defence and Response*. The United Nations Institute for Disarmament Research. <https://doi.org/10.37559/GEN/21/01>, 11.

³ Slupska, J. (2019). Safe at Home: Towards a Feminist Critique of Cybersecurity. *St. Anthony's International Review*, 15(1), 83–100. Available at SSRN: <https://ssrn.com/abstract=3429851>, 84.

⁴ Shafiqat, N., & Masood, A. (2016). Comparative Analysis of Various National Cyber Security Strategies. *International Journal of Computer Science and Information Security*, 14(1), 132.

⁵ Shoker, S. (2020). Making Gender Visible in Digital ICTs and International Security. Report submitted to Global Affairs Canada. <https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf>

⁶ Maschmeyer, L., Deibert, R. J., & Lindsay, J. R. (2021). A tale of two cybers—How threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology & Politics*, 18(1), 1–20. <https://doi.org/10.1080/19331681.2020.1776658>, 1.

⁷ Ibid.

⁸ Slupska, J., & Tanzer, L. M. (2021). Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. In J. Bailey, A. Flynn, & N. Henry (Eds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald, 681.

fail to include the societal level or that are exclusively technical (i.e., focused on systems and infrastructure) are fundamentally disadvantaged in capturing the gendered dimensions of cybersecurity.

Applying a human rights lens to this issue produces a human-centric approach to cybersecurity. A human-centric (in this context often referred to as human-rights based) allows us to conceptualize cybersecurity more holistically, addressing the technological, social and legal aspects.⁹ Beyond focusing on conventional national security interests such as protecting critical infrastructure, this also allows to include digital rights (such as the right to privacy and freedom of expression in the context of digital data and online platforms, or the right to internet access), and other threats to human rights and democracy facilitated by technology (such as online violence and disinformation) as a subject of cybersecurity.

A human-centric definition of cybersecurity emphasizes the direct impact of cyber threats to individuals instead of states or businesses and sees threats coming from a range of actors, both state and non-state.¹⁰ This represents a crucial shift in the distribution of roles of the individual and the state: The state can intentionally or unintentionally be a source of cyber threats. Conversely, individuals and non-state actors are no longer just threat actors but primal recipients of cyber protection. Here, the human-centric approach emphasizes the cybersecurity needs of citizens and civil society organizations as active contributors to cybersecurity interventions. This is sometimes referred to as the 'citizen co-production of cybersecurity'¹¹ or a 'whole-of-society'¹² approach.

From a gender perspective, the human-centric approach, an inclusive approach to implementing cybersecurity norms, does not rely solely on government or business actors to identify cyber threats and interventions. It is a crucial basis to access women's experiences in cyberspace and the knowledge and expertise of women's rights organizations, thus better-incorporating women's cybersecurity needs and rights in public policy. Centering the assessment of cyber threats around individuals acknowledges that citizens experience cyber threats and harms differently, depending on their gender identity and other demographic characteristics. It recognizes that cyber attacks may disproportionately harm those in vulnerable and marginalized positions and that these structural inequalities should be reflected in the design of cybersecurity interventions.

The human-centric approach also has implications for the subject of cybersecurity. A state-centric approach that focuses on a state's security instead of the interests of citizens and users and on resourcing strategic and military aspects of cyberspace. In addition to the protection of systems and infrastructure, a human-centric approach to cybersecurity, thus, also aims to build society-wide social resilience beyond the merely technical.

⁹ <https://www.apc.org/en/pubs/apc-policy-explainer-human-rights-based-approach-cybersecurity>

¹⁰ Deibert, R.J. (2018). Toward a human-centric approach to cybersecurity. *Ethics & International Affairs*, 32(4), 411-424.

¹¹ Chang, L. Y., Zhong, L. Y., & Grabosky, P. N. (2018). Citizen co-production of cybersecurity: Self-help, vigilantes, and cybercrime. *Regulation & Governance*, 12(1), 101-114.

¹² Thinyane, M. & Christine, D. (2020), Co-production of Cyber Resilience in Asia and the Pacific: Abridged Preliminary Report, United Nations University Institute in Macau.

2.2 Gender and Cybersecurity

Women and other marginalized groups in society experience and use the cyberspace differently. They are often disproportionately harmed by cyber threats and encounter additional, gendered forms of cyberviolence. Digital technologies can carry existing gender norms and gendered systems of oppression and abuse from the offline world into digital spaces.¹³ They can aggravate and aggregate existing forms of threat and abuse, even create entirely new ones,¹⁴ and carry offline consequences for women, creating a continuum of gendered violence.¹⁵ Additionally, already vulnerable groups often face barriers or further risks when accessing or applying cybersecurity mechanisms. While the experience of cyber threats and cybersecurity interventions can be different based on gender, this difference is not commonly represented in the policies and practices around cybersecurity.¹⁶

To address this, cybersecurity threat assessments should consider how traditional cybersecurity threats, such as attacks on critical infrastructure, have gendered impacts but also emphasize non-traditional cybersecurity threats that disproportionately affect women and women's rights organizations. Such threats that have traditionally been underrepresented in cybersecurity policy fora, on the multilateral as well as regional and national levels, but that are particularly relevant from a gender perspective are online gender-based violence (GBV), surveillance and privacy violations, misogynistic and anti-LGBTQI+ radicalization and mobilization online, as well as gendered aspects of cybercrime such as human trafficking online.

Gender-based Violence in Cyberspace

Women are more often or more severely affected by digital violence in the form of harassment, surveillance and violations of privacy, doxing, cyber-stalking, disinformation, and the spread of fake news and false information about individuals, as well as non-consensual dissemination of intimate images and unauthorized pornography.¹⁷

¹³ Yao, S. (2019). Gender violence online. In L. Shepherd, *Handbook on Gender and Violence* (pp. 217–230). Edward Elgar Publishing. <https://doi.org/10.4337/9781788114691.00022>, 221.

¹⁴ Yao, S. (2019). Gender violence online. In L. Shepherd, *Handbook on Gender and Violence* (pp. 217–230). Edward Elgar Publishing. <https://doi.org/10.4337/9781788114691.00022>, 219.

¹⁵ Brown, D., & Pytlak, A. (2020). *Why Gender Matters in International Cyber Security*. Women's International League for Peace and Freedom.

¹⁶ Millar, K., Shires, J., & Tropina, T. (2021). *Gender Approaches to Cybersecurity: Design, Defence and Response*. The United Nations Institute for Disarmament Research. https://doi.org/10.37559/GEN/21/01_7

¹⁷ Ibid; Brown, D., & Pytlak, A. (2020). *Why Gender Matters in International Cyber Security*. Women's International League for Peace and Freedom. https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf, 13-14.; Shoker, S. (2020). *Making Gender Visible in Digital ICTs and International Security*. Report submitted to Global Affairs Canada. <https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf>; Yao, S. (2019). Gender violence online. In L. Shepherd, *Handbook on Gender and Violence* (pp. 217–230). Edward Elgar Publishing. <https://doi.org/10.4337/9781788114691.00022>, 218.

Cybersecurity and Radicalization

Digital spaces can also breed radicalization in men and boys, leading to online and offline violence against women.¹⁸ Online anti-gender or anti-women radicalization and online violent radicalization, are in many cases, deeply intertwined. Forms of violent radicalization that are considered more traditional or mainstream threats to security use anti-gender and anti-women rhetoric to target men and boys, as a first step in the progression to violent radicalization. Thus, the concurrent consideration of both forms of radicalization as cybersecurity issues is crucial for understanding and addressing each. In these cases, digital spaces serve as platforms for the further creation and dissemination of gender-based cyber threats.

Gendered Risks of Emerging Technologies

Some digital technologies facilitate the emergence of new and gendered cyber threats. For example, systems using artificial intelligence and machine learning can be gender-biased both intrinsically (in terms of design) and extrinsically (by using gender-biased data).¹⁹ Synthetic media technologies such as 'deep fakes' have been used to superimpose false images of women in unauthorized pornography and other false depictions.²⁰ Smart devices intended for use inside homes and smart devices with location-tracking capabilities can also be used as a tool for gender-based and intimate partner violence.²¹

In these cases, digital technologies are not inherently harmful to women, but have the potential to create gendered cyber threats. When the potential for such gendered cyber risks is not considered in the design of technology, the burden of cybersecurity falls on the female user, who may not have the tools or literacy to address them on an individual level.²²

It is important to recognize that many cutting-edge technologies do not carry inherent gendered risks by design, and can theoretically be used to address gender-based needs. In other cases, cutting-edge technologies are used in conflict contexts to address human-level risks and threats – in ways that serve to highlight and address the impacts of conflict and crisis that disproportionately affect women. For example, digital technologies are used to monitor and record violence, human rights violations,²³ and the destruction of homes, lands and properties in conflict contexts.²⁴ GNWP and ICT4P's previous research

¹⁸ Shoker, S. (2020). Making Gender Visible in Digital ICTs and International Security. Report submitted to Global Affairs Canada. <https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf>.

¹⁹ Wellner, G., & Rothman, T. (2020). Feminist AI: Can We Expect Our AI Systems to Become Feminist? *Philosophy & Technology*, 33(2), 191–205. <https://doi.org/10.1007/s13347-019-00352-z>.

²⁰ Wagner, T. L., & Blewer, A. (2019). "The Word Real Is No Longer Real": Deepfakes, Gender, and the Challenges of AI-Altered Video. *Open Information Science*, 3(1), 32–46. <https://doi.org/10.1515/opis-2019-0003>

²¹ Slupska, J. (2019). Safe at Home: Towards a Feminist Critique of Cybersecurity. *St. Anthony's International Review*, 15(1), 83–100. Available at SSRN: <https://ssrn.com/abstract=3429851>.

²² Millar, K., Shires, J., & Tropina, T. (2021). Gender Approaches to Cybersecurity: Design, Defence and Response. The United Nations Institute for Disarmament Research. <https://doi.org/10.37559/GEN/21/01>, 18-19.

²³ Hofstetter, J.-S. (2021). Digital Technologies, Peacebuilding and Civil Society. Addressing Digital Conflict Drivers and Moving the Digital Peacebuilding Forward. Institute for Development and Peace. https://www.uni-due.de/imperia/md/content/inef/ir114_hofstetter_final_web.pdf

²⁴ For more information on such uses of cutting edge technologies: 'Guardians of the Records' Lab, based in Canada, conducts research on the use of cutting edge technologies by grassroots actors in conflict and crisis contexts: <https://blockchain.ubc.ca/research/guardians-record-lab>

on WPS and Human Rights in the Digital Age further explore such use cases of cutting-edge technologies.

Human Trafficking and Other Threats to Human Security

Human trafficking has been acknowledged as a gendered security risk due to its roots in patriarchal social inequalities, and the reality that most victims are women. There is a growing awareness amongst public policy institutions that its locus delicti is shifting more and more to cyberspace. Despite this, human trafficking is largely absent from cybersecurity discussions, even in the context of multilateral or national cybercrime fora. Besides its gendered implications, human trafficking should be considered a particularly severe cybersecurity threat, as it often targets women in vulnerable conditions, including forced migration and armed conflict. Recent examples of Ukrainian refugees have shown that online platforms and social media groups seemingly set up for citizen-to-citizen emergency help for refugees were misused as Tinder for sex traffickers.²⁵

Gendered impacts of Conventional Cyber Threats

Other cyber threats recognized by conventional understandings of cybersecurity, and are not gendered in their origin, still carry differentiated gendered impacts. For example, internet shutdowns like the 2016 Russian shutdown of the internet in

Crimea or shutdowns resulting from 2016 cyber attacks in Libya, did not target women specifically. However, they caused women to lose their means of external communication and access to critical information, crucial tools to ensure their personal safety outside the home, platforms for informal work and e-commerce with detriments for their economic well-being, and access to other online services such as education.²⁶ Data breaches may also carry differentiated gendered impacts – for example, in cases where breaches of medical data exposed the personal information of medical professionals providing reproductive services and care, and of the patients receiving them.²⁷

Limited Access to Cybersecurity Provisions

In many cases, reporting and accountability mechanisms for digital violence particularly affecting women are absent, or not up to par with mechanisms addressing offline threats and violence.²⁸ Where legal mechanisms to address cyber threats do exist, access to these mechanisms (e.g., going to court, building a case, or interacting

²⁵ Townsend, M. (2022). UK's Homes for Ukraine scheme risks operating as 'Tinder for sex traffickers', say charities. *The Guardian*. <https://www.theguardian.com/uk-news/2022/mar/26/uk-homes-for-ukraine-scheme-risks-operating-as-tinder-for-sex-traffickers-say-charities>

²⁶ Brown, D., & Pytlak, A. (2020). Why Gender Matters in International Cyber Security. *Women's International League for Peace and Freedom*. https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf, 8-12.

²⁷ Ibid.

²⁸ Fal Dutra Santos, A., Buzatu, A.-M., Lakehal, D., Pourmalek, P., & Zelenanska, M. (2021). Women, Peace and Security and Human Rights in the Digital Age: Opportunities and Risks to Advance Women's Meaningful Participation and Protect their Rights. *Global Network of Women Peacebuilders*. <https://gnwp.org/wp-content/uploads/PolicyBriefGNWP-2021c.pdf>, 24.

with law enforcement) is also limited by gender-based barriers.²⁹ There is also a gender divide in terms of access to knowledge and financial resources needed for digital literacy, access to information on data privacy, and access to secure digital infrastructure.

Participation in Technology and Policy Design Processes

From the creation and design of digital technologies, to conceptualizing threats to security in the digital realm, to mitigating and responding to cyber threats, gender has applications to nearly all dimensions of cybersecurity policy formulation and technology design processes. Thus, the participation of women in the development of digital technologies, the cyber workforce and industry, as well as cybersecurity diplomacy and policymaking, is another important area for considering gender in cybersecurity. The lack of representation of women in the creation of digital technologies translates to less gender sensitivity in designing technology and increases the likelihood of 'hardcoding' existing biases, including gender bias, into technology.³⁰ Beyond business and industry, women are also underrepresented in policy processes and diplomacy related to cybersecurity.³¹

2.3 Intersectionality and What We Mean by 'Women' and 'Gender'

While gendering cybersecurity policy through WPS sets a particular focus on women and women's rights organizations, the analysis and recommendations delivered in this report also apply to other marginalized groups, as they often face the same vulnerabilities in cyberspace, and underrepresentation of their rights and needs in cybersecurity policies.

Moreover, the term 'gender' encompasses a diverse set of gender identities and should not be used to reinforce stereotypical gender roles or a binary understanding of gender. Analyzing cybersecurity through a gender perspective should be done through an intersectional lens, which acknowledges that besides gender identity, other characteristics of discrimination, such as sexual orientation, race, nationality, and legal status, can intensify vulnerabilities or create new ones.

A gender perspective not only means to look at women's and other marginalized groups' vulnerabilities, but it also encompasses men's and boys' roles and how patriarchal structures shape institutions, policies, and practices. Policies that address women's safety are often grouped with measures addressing child protection, which is an expression of a paternalist system that treats women as minors in need of protection and denies them agency.³² Cybersecurity policies addressing women and children should thus be treated separately.

²⁹ Millar, K., Shires, J., & Tropina, T. (2021). Gender Approaches to Cybersecurity: Design, Defence and Response. The United Nations Institute for Disarmament Research. <https://doi.org/10.37559/GEN/21/01>, 43-44.

³⁰ Brown, D., & Pytlak, A. (2020). Why Gender Matters in International Cyber Security. Women's International League for Peace and Freedom. https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf, 15; Millar, K., Shires, J., & Tropina, T. (2021). Gender Approaches to Cybersecurity: Design, Defence and Response. The United Nations Institute for Disarmament Research. <https://doi.org/10.37559/GEN/21/01>, 5-6.

³¹ Slupska, J. (2019). Safe at Home: Towards a Feminist Critique of Cybersecurity. *St. Anthony's International Review*, 15(1), 83-100. Available at SSRN: <https://ssrn.com/abstract=3429851>, 87.

³² Dorokhova, E. et al (2021) Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach. DCAF. https://www.dcaf.ch/sites/default/files/publications/documents/CyberVAWG_in_WB.pdf

2.4 Conflict-Sensitive Cybersecurity and 'Do No Harm'

There is a growing awareness among cybersecurity policymakers and experts that cybersecurity measures implemented by states to prevent and prosecute cyber harms, with the intention of making cyberspace safer for citizens, can cause more harm than good. State cybersecurity interventions, including well intended legislation to fight disinformation or data gathering in the justice system to fight cybercrime, might have unintended negative consequences. This not only puts already vulnerable cybersecurity recipients at further risk, it also threatens to undermine citizens' trust in digital public services. Moreover, the inherent trade-off between national security interests and the protection of human rights such as data privacy raises questions on whether national security institutions should be leading efforts to protect rights in cyberspace, as is often the case in the context of national cybersecurity policy-making. On the inter-state level, the militarization of cybersecurity threatens to increase political tensions and lead to an escalation of conflict. It also neglects the severe human suffering cyber attacks can cause – even though they are seen as less violent options to conventional armed conflict.

Cybersecurity policymaking, in general, should, therefore, incorporate the principle of conflict-sensitivity, and each cybersecurity measure should undergo its own context-specific 'do no harm' assessment. In the context of the harmful impacts of cybersecurity interventions, women and other vulnerable groups face particular and often more severe risks. For example, in the context of technology-facilitated domestic violence, victims are often forced to share sensitive private data with law enforcement, which might put them in an even more vulnerable position. For undocumented or otherwise 'illegal' immigrants, sharing sensitive information with authorities can have severe and direct consequences for safety, and brings about risks of deportation. These examples show the necessity of incorporating an intersectional gender perspective to 'do no harm' assessments of cybersecurity interventions.

What poses a more complex problem in the context of the negative impact of cybersecurity interventions is when the state itself abuses such interventions for political purposes and becomes a cyber threat actor. For example, by silencing political opponents through censoring online content, spreading online propaganda, using surveillance technologies, or using the fight against disinformation as a pretext for prosecution. In these cases, civil society plays a crucial role as an alternative provider of cybersecurity, providing cybersecurity capacity-building for citizens, advocating for digital human rights, and holding the government accountable for abusive behavior. The possibility that the state can be a cyber threat actor also highlights the importance of international cyber norms; the need to expand them to incorporate cybersecurity threats, and apply responsible state behavior not only on the inter-state level but in state-citizen relations.



3. OVERVIEW OF KEY POLICIES AND DISCUSSIONS AT NATIONAL AND INTERNATIONAL LEVELS

3.1 Gender and Cybersecurity at the Multilateral Level

3.1.1 Multilateral Cybersecurity Fora

Much of the current discourse around the relevance of gender to cybersecurity has focused on the international level. The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UN GGE), established in 2004, and the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG), created in 2018, are the primary bodies responsible for discussions of international norms and standards on cybersecurity by states at an international level. The GGE and the OEWG recognized the “importance of narrowing the gender digital divide and ensuring gender non-discrimination in cyberspace”. At the same time, only the most recent of four UN GGE consensus reports mention gender.³³

Delegations participating in the OEWG have increasingly promoted a gendered perspective and gender-sensitivity in norms of cybersecurity – although most references were made only in the context of women’s participation.³⁴ Some delegations have gone further in connecting the need for more gender sensitivity in cybersecurity with the WPS. For example, Canada’s proposal for the 2019-2020 OEWG report makes several references to gender,³⁵ its proposal for the 2021-2025 OEWG advances this conversation by discussing how gender can be mainstreamed in the OEWG’s work raising issues such as gender-related threats, including “how internet shutdowns and data breaches affect women and the LGBTQ community differently,” gender mainstreaming in national cyber strategies, and making suggestions on how to gender mainstream capacity-building.³⁶ While proposals submitted to the 2021 OEWG report already called for gender-disaggregated data, measures to address the digital divide and establishing links to the WPS agenda, these demands were not taken up by in the final document due to a lack of consensus among member states.³⁷ However, what indicates progress regarding the better recognition of gender, is that the resolution adopted by the First Committee of the UNGA in November 2022, which proposes to establish a Programme of Action on cybersecurity (as a permanent, inclusive, action-

³³ Fal Dutra Santos, A., Buzatu, A.-M., Lakehal, D., Pourmalek, P., & Zelenanska, M. (2021). Women, Peace and Security and Human Rights in the Digital Age: Opportunities and Risks to Advance Women’s Meaningful Participation and Protect their Rights. Global Network of Women Peacebuilders. <https://gnwp.org/wp-content/uploads/PolicyBriefGNWP-2021c.pdf>, 26.

³⁴ Millar, K., Shires, J., & Tropina, T. (2021). Gender Approaches to Cybersecurity: Design, Defence and Response. The United Nations Institute for Disarmament Research. https://doi.org/10.37559/GEN/21/01_2; Pytlak, A. (Ed.). (2020). Cyber Peace and Security Monitor. Women’s International League for Peace and Freedom.

<https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.7.pdf>, 3, 15.

³⁵ Canada’s Proposal for the Report of the 2019-20 United Nations Open-Ended Working Group on “Developments in the Field of Information and Telecommunications in the Context of International Security.” (n.d.). Retrieved January 17, 2021, from <https://www.un.org/disarmament/wp-content/uploads/2019/09/canadian-position-paper-oewg-en.pdf>

³⁶ Canada’s Proposal for the Report of the 2021-25 United Nations Open-Ended Working Group on “Developments in the Field of Information and Telecommunications in the Context of International Security. Annex I.” Retrieved October 12, 2022, from <https://documents.unoda.org/wp-content/uploads/2021/12/Canadian-position-paper-2021-25-OEWG-final-Dec-6-Annex-Gender-Considerations.pdf>.

³⁷ Sharland, L., Goussac, N., Currey, E., Feely, G., & O’Connor, S. (2021). System Update: Towards a Women, Peace and Cybersecurity . UNIDIR, 18.

oriented mechanism to follow the OEWG 2021-2025 proceedings) emphasizes the importance of narrowing the “gender digital divide” and of promoting the participation and leadership of women in decision-making processes.³⁸

It is important to note that the OEWG, which is considered to be the more inclusive of the two bodies, is still exclusionary to some extent. Only very few non-governmental organizations participated in past proceedings, with many who sought permission to attend being denied access. Furthermore while organizations such as Women's International League for Peace and Freedom have been active in promoting a gender-sensitive approach at the OEWG,³⁹ the notable exclusion of many civil society organizations likely hinders progress in recognizing the relevance of gender to cybersecurity.

The UN Security Council is increasingly acknowledging the relevance of cyberspace to international security, holding meetings on “Cybersecurity and International Peace and Security” in November 2016, March 2017, and in August 2020 and organizing its first official United Nations Security Council (UNSC) open debate on maintaining international peace and security in cyberspace in June 2021. These discussions, however, largely lacked a gender lens.

In the context of multilateral efforts to counter cybercrime, human-centric approaches to cybersecurity and calls, as well as measures to integrate a gender perspective, have taken much more prominent and concrete forms. This has especially been the case in the recently held negotiations on a new UN treaty on cybercrime. In 2019, the UN General Assembly decided to establish an Ad Hoc Committee to develop an international convention on countering the use ICTs for criminal purposes.⁴⁰ The committee convened UN Members State delegations three times since January 2022 to negotiate the future cybercrime convention. Many state and non-state representatives emphasized the need to include provisions for the protection of vulnerable groups in cybercrime policymaking, with many sharing proposals on how to address GBV and on how to gender mainstream the negotiation process and the convention itself.⁴¹

3.1.2 Multilateral Gender and Human Rights Documents

The presence of gender in ongoing multilateral processes and key documents addressing cybersecurity highlight a shallow engagement with gender and gender-specific issues. In this context, it is valuable to determine the extent to which key bodies relevant to issues of gender and human rights, and the documents they produce, engage with cybersecurity. Human rights frameworks are of particular significance, as they are concerned with experiences at the human level, much like human-centric approaches to cybersecurity. Among the issue areas at the intersection of cybersecurity and gender identified in Section 2 of this report, online

³⁸ UN GA Draft Resolution, Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security, <https://digitallibrary.un.org/record/3991743?ln=en>

³⁹ Pytlak, A. (Ed.). (2020). Cyber Peace and Security Monitor. Women's International League for Peace and Freedom. <https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.7.pdf>, 2.

⁴⁰ UN GA Resolution 74/247, Countering the use of information and communications technologies for criminal purposes.

⁴¹ On gender mainstreaming, see for example: <https://chathamhouse.souttron.net/Portal/Public/en-GB/RecordView/Index/191233>

GBV is most commonly addressed, followed by issues of misinformation and disinformation, and radicalization.

Several resolutions of the Human Rights Council (HRC) address technology in the context of human rights, of which only two address online gender-based violence.⁴² Two reports of the Special Rapporteur on Violence Against Women address the intersections of gender and technology and online gender-based violence.⁴³ Even in cases where the relevance of gender is recognized, the language and framing of cybersecurity are notably absent. The Special Rapporteur's 2018 report on online violence against women is the only exception. While cybersecurity is not mentioned, related language such as "cyber-violence," "cyber abuse," "cyberbullying," and "cyberstalking" are used to frame gendered issues in cyberspace.

HRC resolution 49/21 (2022) on disinformation and human rights recognizes the role of gender in relation to misinformation and disinformation, and the specific targeting of women readers, including women human rights defenders, advocates, politicians, and journalists with online disinformation campaigns. While cybersecurity language is used elsewhere in the resolution, it is not used when discussing women or gender. The report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression on "[d]isinformation and freedom of opinion and expression" similarly identifies a gendered dimension to disinformation and a need for gendered perspectives in addressing misinformation and disinformation. However, the report is grounded in human rights language and does not take a cybersecurity approach to the issue. The Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism (2016) includes a dedicated section on "violent extremism and gender". Still, it does not engage with the gendered underpinnings of online radicalization and violent extremism.

With the objective of examining international instruments specifically focused on women's rights, the documents produced in connection to the Convention on the Elimination of Discrimination Against Women (CEDAW) were surveyed. Among 949 State Party Reports submitted to the CEDAW and the CEDAW Committee's Concluding Observations for the period 1982-2021, only 20 (2%) use the language of cybersecurity. In most cases, cybersecurity is addressed in the context of GBV, including relevant legislation on cybercrime. This gap is especially important to address given the CEDAW Committee's General Recommendation No. 30 on "women in conflict prevention, conflict and post-conflict situations".⁴⁴

In taking a rights-based approach, many of the above documents avoid language that securitizes the issues at hand. Cybersecurity language and framing thus may also be excluded as a result of a concern for the securitization of gender or human rights issues. Here, a human-centric framing of cybersecurity issues can be beneficial in two ways. First,

⁴² HRC Resolutions 21/7 (2016), 33/2 (2016) and 38/7 (2018), among other resolutions addressing technology: 12/16 (2009), 20/8 (2012), 23/2 (2013), 26/13 (2014), 28/16 (2015), 31/7 (2016), 33/2 (2016), 32/13 (2016), 34/7 (2017), 37/2 (2018).

⁴³ Reports of the Special Rapporteur on Violence Against Women on "Promotion, protection and enjoyment of human rights on the Internet: ways to bridge the gender digital divide from a human rights perspective" (2017) and "Violence against women, its causes and consequences on online violence against women and girls from a human rights perspective" (2018).

⁴⁴ For more information on the experiences of women peacebuilders with online gender-based violence, refer to Pourmalek, P., & Fal Dutra Santos, A. (2022). Preventing Violence in the Digital Age: Women Peacebuilders and Technology Facilitated Gender-Based Violence. In M. Garrido (Ed.), Mapping Online Gender-Based Violence. UPEACE. <https://www.upeace.org/files/Publications/Garrido-Mapping%20online%20gender-based%20violence%20FULL%20BOOK.pdf>

a focus on human-level experiences as the angle for outlining the impact of large-scale phenomena such as online GBV, misinformation and disinformation, and violence radicalization – allowing for mutual reinforcement of human rights and human security approaches. At the same time, employing a human-level perspective pushes back against dominant approaches to cybersecurity that focus on the state level exclusively, and often use state security as a justification for the violation or limitation of human rights. Section 3.2 will further discuss the value of the WPS as a tool rooted in both security and human rights-oriented approaches, and the value it holds for gendering current approaches to cybersecurity.

3.2 Gender and Cybersecurity at the National Level

3.2.1 Gender in National Cybersecurity Policies

At the state level, National Cyber Security Strategies are key policy documents designed to address the cybersecurity landscape facing a country. National Cyber Security Strategies aim to maximize the benefits of digitalization and ICTs, particularly for social and economic welfare, and address potential cyber risks and threats to cybersecurity.⁴⁵ There is an increased recognition of these strategies as central to international peace and security. The International Telecommunication Union (ITU) reports that 114 out of 193 of its Member States currently have a National Cyber Security Strategy.⁴⁶ The slow but increasing recognition of gender in the interstate discourse on norms of cybersecurity does not necessarily translate to a similar recognition at the state level.

The protection of critical infrastructure, partnerships with the private sector, international cooperation, and better intra-government cooperation are common themes across different National Cyber Security Strategies.⁴⁷ A human-centric or human-rights-based approach to cybersecurity, which could indirectly capture gendered dimensions of cybersecurity, is still underrepresented in NCS. Only 34 NCS make some reference to human rights, of which only two advocate for a human rights-based approach to cybersecurity. Moreover, only 14 NCS explicitly mention gender or women and most do so solely referencing the gender gap in the technology and cybersecurity industry, falling short in addressing gender-specific cybersecurity concerns and women's societal cyber resilience and human rights online.

One NCS mentions combating online violence against women as a strategic priority of their NCS, dedicating a whole section to 'gender rights online', including a concrete plan for implementation and defining measures of success. Proposed interventions include establishing a multi-stakeholder forum for the development of protecting

⁴⁵ Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy (OECD Digital Economy Papers No. 211; OECD Digital Economy Papers, Vol. 211). (2012). <https://doi.org/10.1787/5k8zq92vdgtl-en>, 5.

⁴⁶ International Telecommunication Union, "National Cybersecurity Strategies Repository", n.d., <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx>.

⁴⁷ Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy (OECD Digital Economy Papers No. 211; OECD Digital Economy Papers, Vol. 211). (2012). <https://doi.org/10.1787/5k8zq92vdgtl-en>: 6-7. Dupont, B. (2012). The proliferation of cybersecurity strategies and their implications for privacy. In K. Benyekhlef & E. Mitjans (Eds.), *Circulation internationale de l'information et sécurité* (pp. 67–80). Éd. Thémis, 6-8.

gender rights online, support to promote advocacy of relevant organizations, collaboration with internet service providers, regulatory agencies, and owners of online platforms, and establishing and promoting reporting mechanisms for online violence against women. Notably, the strategy was developed consulting a broad spectrum of stakeholders representing the public sector, private sector, academia, and civil society, including women's rights organizations, on numerous occasions and involving them early in the design process.⁴⁸

Gender sensitivity is also far from being recognized as a good or common practice in developing National Cyber Security Strategies. For example, the 2021 "Guide to Developing a National Cybersecurity Strategy," developed by the ITU in partnership with a range of non-governmental actors, international organizations, and private companies, makes only one reference to gender – in the context of diversity in the cybersecurity sector.⁴⁹

3.2.2 Cybersecurity in WPS NAPs

The reference to cybersecurity in most WPS NAPs is limited to the use of the technologies as tools for peacebuilding or to a lesser extent as a source of violence and insecurity. As discussed in GNWP and ICT4P's previous research on ICTs and peacebuilding, both digital and conventional technologies are increasingly present in, and necessary for, successful women and youth-led peacebuilding.⁵⁰ The increasing presence of language around technology in NAPs on WPS is reflective of this shift in the practice of peacebuilding, which runs in parallel with the growing ubiquity of technology in all aspects of life. At the same time, an increasing engagement with digital technologies further necessitates meaningful engagement with cybersecurity as risks and threats emerging from cyberspace grow more pervasive – not only for women and youth peacebuilders but for all women and girls. Of 103 NAPs on WPS in force as of August 2022,⁵¹ only four make specific reference to cybersecurity, and two reference cybersecurity within the Plans' Implementation priorities – under the WPS pillars of prevention and protection.

It is important to flag that the entrenchment of digital technologies, the internet, and cyberspace into the daily lives of all people – including women and girls – has taken place at an accelerated rate in recent years. Thus, policies and plans with a multi-year drafting process and implementation window, such as NAPs on WPS, may always fall behind in engaging with the contemporary role of digital technologies. If this is the case, the next generation of NAPs on WPS, many of which will be released in the upcoming years, can be expected to have a more detailed engagement with the role of digital technologies, and, crucially, with cybersecurity.

⁴⁸ Ajijola, A.-H., & Allen, N. D. F. (2022, March 8). African Lessons in Cyber Strategy. Africa Center for Strategic Studies. <https://africacenter.org/spotlight/african-lessons-in-cyber-strategy/>

⁴⁹ International Telecommunication Union. (2021). Guide to Developing a National Cybersecurity Strategy. <https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/2021-ncs-guide.pdf>

⁵⁰ Fal Dutra Santos, A., Buzatu, A.-M., Lakehal, D., Pourmalek, P., & Zelenanska, M. (2021). Women, Peace and Security and Human Rights in the Digital Age: Opportunities and Risks to Advance Women's Meaningful Participation and Protect their Rights. Global Network of Women Peacebuilders. <https://gnwp.org/wp-content/uploads/PolicyBriefGNWP-2021c.pdf>

⁵¹ Resources: Global Map of National Action Plans. (n.d.). WPS Focal Points Network. Retrieved October 12, 2022, from <https://wpsfocalpointnetwork.org/resources/>

3.3 How the WPS Framework Can be Used to Re-Design Cybersecurity Policies

For many states, cybersecurity occupies a space on the policy agenda as a critical emerging threat to security, both domestically and internationally. This is due to the ubiquitous presence of technology in all aspects of human life and statecraft, and the increasingly common occurrence of cyber threats and attacks. Given the prioritization of cybersecurity, current policy discourse on cybersecurity is focused on establishing domestic and international norms of cybersecurity. This window provides an opportunity to promote progressive cybersecurity norms. Here, a human-centric, gender-sensitive, and conflict-sensitive approach is needed to prevent the entrenchment of norms that recognize the state level exclusively and equate cybersecurity to state security.

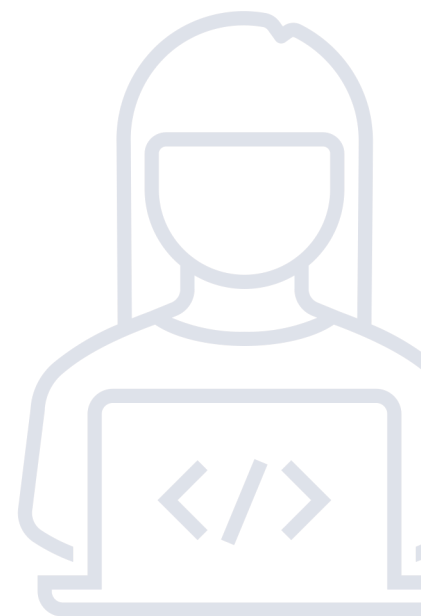
Based on the framing of cybersecurity provided thus far, this report argues that this window provides an opportunity to promote progressive cybersecurity norms. Here, a human-centric, gender-sensitive, and conflict-sensitive approach is needed to prevent the entrenchment of norms that recognize the state level exclusively, and equate cybersecurity to state security.

The impact of cyberspace on individuals and communities at the human level is significant for two reasons. Threats, risks, and attacks emerging from cyberspace bring about real harm to humans and undermine the human security of the individual. At the same time, these human-level impacts can indirectly undermine the security of the state. The Women, Peace and Security agenda is a valuable tool for re-designing policies and approaches to cybersecurity toward this end, for four reasons:

1. Given its origins, the WPS agenda captures the inherent connection between cybersecurity and conflict, while not neglecting the applicability of cybersecurity in peacetime;
2. The WPS agenda contributes a gender lens to cybersecurity, which can explain how socially constructed norms and identities determine the specific and differentiated impacts of cyber threats and risks on individuals;
3. WPS is a well-established agenda that legitimizes the importance of the human level of security, and can be used to reinforce human-level approaches to cybersecurity; and
4. WPS can address the specific ways in which threats and risks emerging from cyberspace undermine peace and peacebuilding efforts, erode social cohesion, and fuel and produce conflict.

Each pillar of the WPS agenda can lend itself directly to this advocacy. A 2022 advocacy brief on adopting a WPS lens in cybersecurity, produced by UN Women, provides the following:

- Participation and prevention: “ensuring and promoting women’s leadership, participation and representation in technology and cybersecurity planning, design and governance and relevant law enforcement efforts, in line with WPS recommendations”;



- Prevention: “preventing gender-based cybersecurity threats, online harms, and cyber-enabled crimes through conflict-sensitive and gender-responsive approaches”;
- Protection of rights: “protecting women’s human and digital rights while ensuring their safety from gender-based cybersecurity threats, online harms and cyber-enabled crimes, both online and offline”; and
- Relief and recovery: “relief and recovery efforts in post-conflict / crisis contexts should use technology in a conflict-sensitive, gender-responsive and survivor-centred manner.”

Better integration of WPS and cybersecurity will thus allow for the promotion of more progressive norms of cybersecurity that recognize and address the experiences of individuals alongside that of the State. In turn, the framework and language of cybersecurity allow the WPS agenda, including NAPs on WPS, to recognize and address the threats posed by digital technologies and cyberspace to peace, and women-led peacebuilding.

4. GENDER AND CYBERSECURITY IN NATIONAL POLICIES: SYNERGIES BETWEEN NCS AND WPS NAPs

4.1 Gender-sensitivity in National Cybersecurity Policies

NCSs take various forms, and their depth and scope vary depending on the country’s capacity to develop cybersecurity policies and instruments. Significant disparities exist between national contexts regarding government compositions, legal frameworks, and political strategies, which complicate the utility of universal recommendations on incorporating gender into NCS. Moreover, women’s digital rights and vulnerabilities to cyber threats on the national level, when addressed, often fall into other policy or legislative domains such as online safety, or defamation and harassment laws. However, addressing these issues in the context of National Cybersecurity Strategies would allow governments to better coordinate the incorporation of a gender perspective in these individual laws and policies. The NCS approach also increases governments’ ability to allocate adequate resources and expertise for the further development and implementation of gender-sensitive legal frameworks, by framing women’s digital rights and cyber vulnerabilities as national security priorities.

NCS usually include three key components.⁵² 1) They define the high-level objectives, principles, and priorities that guide national responses to cyber threats, 2) they provide an overview of the relevant stakeholders and their respective roles and responsibilities, and 3) they describe the steps, programs, and initiatives that a country will undertake to increase its cybersecurity and resilience. Here, integrating the WPS angle is crucial, as it allows governments to set gender equality in cyberspace as a national security priority. The integration of WPS also supports the inclusion of women and women’s rights organizations as relevant cybersecurity stakeholders. It ensures that women’s cybersecurity needs and rights are not neglected when designing concrete cybersecurity initiatives.

⁵² Guide to Developing a National Cybersecurity Strategy. (2021). International Telecommunication Union (ITU). <https://ncsguide.org/wp-content/uploads/2021/11/2021-NCS-Guide.pdf>

The following sections provide recommendations for gender mainstreaming the different phases of designing and implementing an NCS. They also discuss why and how to facilitate an open and participatory process in the design and implementation of NCS, with contributions from a society-wide spectrum of stakeholders, especially women's rights groups, and organizations representing other marginalized groups, to ensure gender-sensitive NCS.

4.1.1 Gender Mainstreaming National Cybersecurity Policies

Gender mainstreaming is a strategy to guarantee equality between all genders throughout all public policy and legislation. It has two dimensions that need to be considered in all phases of the policymaking process: Equal representation of all genders, and integrating a gender perspective into the policy content.⁵³

The first dimension addresses the representation of all genders as beneficiaries of cybersecurity policies, as well as their representation in the labor force and the decision-making processes. The second dimension demands a gender-responsive policy, which ensures that the needs of all genders are equally addressed. A basis for this is conducting a gender analysis, which refers to the critical examination of how differences in gender needs, opportunities, and rights "influence how individuals are affected by cyber threats and cybersecurity policy". There are different gender mainstreaming toolkits available that can be used to conduct a gender analysis of national cybersecurity interventions.⁵⁴

Moreover, gender mainstreaming should be applied to all phases of NCS formulation. The 'NCS Guide 2021'⁵⁵ identifies four phases: (1) the initiation, (2) stocktaking and analysis, (3) production of the NCS, and (4) implementation.

1. The initiation phase includes identifying the lead project authority, establishing a steering committee, identifying stakeholders to be involved in the development of the strategy, identifying human and financial resources, and planning the development of the strategy. Here the meaningful inclusion and participation of women and women's rights organizations, as well as government entities working on gender and women's rights, is particularly relevant to set gender equality in cyberspaces as a priority.
2. The second phase entails assessing the national cybersecurity and cyber risk landscape. Applying a gender lens to these assessments is crucial to identify the particular vulnerabilities women face in cyberspace, but also to identify gaps in regulatory frameworks or possibly barriers to the criminal justice system.
3. The third phase spans from drafting the national cybersecurity strategy, to consultation processes with national, regional and international stakeholders, to the formal approval, publishing and promotion of the strategy. In this phase, actively approaching women's rights organizations and providing capacity-

⁵³ What is gender mainstreaming. (n.d.). European Institute for Gender Equality (EIGE). Retrieved October 12, 2022, from <https://eige.europa.eu/gender-mainstreaming/what-is-gender-mainstreaming>

⁵⁴ DCAF's NAPRI toolkit, for example, provides a framework to apply a gender perspective to policy and legislation in the security and justice sector along the categories of needs, access, participation, resources, and impact. <https://issat.dcaf.ch/download/131668/2694399>. On good governance in cybersecurity and gender equality see also Millar, K., Shires, J., and T. Tropina (2022). Gender equality, cybersecurity, and security sector governance. DCAF.

⁵⁵ Guide to Developing a National Cybersecurity Strategy. (2021). International Telecommunication Union (ITU). <https://ncsguide.org/wp-content/uploads/2021/11/2021-NCS-Guide.pdf>

building on national cybersecurity issues and structures can have a crucial impact on their meaningful participation in the consultations.

4. In the implementation phase, gender considerations should be applied to the development of the action plan, the prioritization of initiatives to be implemented, to the allocation of human and financial resources for the implementation. Such considerations can also be applied when setting timeframes and developing metrics and other accountability measures.

A crucial aspect of gender mainstreaming is the implementation of effective accountability mechanisms. Such mechanisms could include regularized gender audits of the gender mainstreaming activities of both the national government entity responsible for NCS and within institutions and departments responsible for the implementation of specific cybersecurity measures. Also ensuring transparent reporting practices and subjecting the implementation of cybersecurity policy to legislative and civilian oversight on a regular basis can help to monitor the gender-sensitivity of these policies.⁵⁶

4.1.2 Inclusive Multi-stakeholder Engagement: Strengthening Civil Society's Role in the Development of NCS and Beyond

Broad and meaningful multi-stakeholder consultations are integral to promoting gender equality. Engaging women and women's rights organizations in the design, implementation and oversight of cybersecurity interventions are crucial in order to incorporate the needs and perspectives of all genders into cybersecurity policymaking.

While many NCS pledge to design their national cybersecurity policymaking inclusively and to adopt a multi-stakeholder approach, the proposed dialogue formats and stakeholder engagement are often limited to public-private exchanges and rarely include stakeholders from civil society, and even less so women's rights organizations. Adopting a more inclusive approach to stakeholder engagement that not only focuses on businesses – as active contributors to cybersecurity interventions as well as entities in need of protection – but also citizens and civil society organizations, would allow governments to better access data on women's cybersecurity needs, and the knowledge and expertise of women's rights organizations.

To strengthen civil society's inclusion as part of the strategy development, good practices range from online surveys administered to national stakeholder groups, to citizen engagement through open forums organized across the country or through open online consultations, and publishing cybersecurity strategy draft papers and requested contributions from stakeholders and making submissions public. This could also include convening a multi-stakeholder workshop to increase awareness among stakeholders about cyber policy issues, and providing a space for stakeholders to discuss their priorities and increase coordination. Other options include organizing training workshops for civil society groups to enable them to engage in cyber policy discussions, and the NCS development process in particular.

⁵⁶ Millar, K. (2022). *What Does it Mean to Gender Mainstream the Proposed Cybercrime Convention? (Draft)*. Chatham House. <https://chathamhouse.soutron.net/Portal/Public/enGB/DownloadImageFile.aspx?objectId=5344&ownerType=0&ownerId=191233>

Beyond developing and designing national strategies, civil society occupies a key role as both the subject and active contributor to cybersecurity. This 'co-production' of cybersecurity is not limited to cybersecurity policy design. Citizens and civil society can also be consulted to develop measures to deter cyber attacks, design cyber capacity-building programs (especially awareness-raising campaigns), and share information about cyber threats. While citizens are primarily framed as recipients of cybersecurity, some states have started to embrace an inclusive approach to cybersecurity, for example, by establishing national cyber incident response teams that accept civilian reporting.⁵⁷ In contrast to citizens or businesses, civil society organizations are rarely considered beneficiaries of cybersecurity policies. While civil society organizations face similar cyber threats experienced by states and businesses, they have far fewer resources at their disposal to defend themselves.⁵⁸ Under the frame of a 'whole-of-society resilience approach,' some states have started to address such cross-sectoral cybersecurity resource inequalities, advocating for cybersecurity capacity-building and emergency response policy that better incorporates the needs of all affected stakeholders, not just actors operating critical infrastructures.⁵⁹

4.1.3 Opportunities and Limitations of NCS as Vehicles for Gender-Sensitive Cybersecurity

Women's digital rights and vulnerabilities to cyber threats are, in most countries, to a certain extent, addressed in not-cybersecurity-specific strategy documents and legislation (e.g., in online safety or data protection laws). Addressing these issues in the context of NCS allows governments to better coordinate the incorporation of a gender perspective in these individual laws and policies, and to allocate adequate resources and expertise for the further development and implementation of gender-sensitive legal frameworks by framing women's digital rights and cyber vulnerabilities as national security priorities. Moreover, adopting a human-centric and gender-sensitive approach to cybersecurity is crucial for addressing gaps in NCS that state- and business-centric approaches create due to a limited view of cyber threat assessments and options for cybersecurity provision, allowing for a more holistic and effective cybersecurity strategy.

There are also limitations to addressing gendered cybersecurity threats through NCS. Developing and implementing NCS, in general, can be a challenging task for many governments. They often fail to do so due to a lack of resources and difficulties coordinating the high numbers of stakeholders involved. Cybersecurity is a society-wide concern that inflicts government-wide responsibilities. Cooperation between different government departments might also prove difficult due to inter-departmental competition and clashing organizational cultures. For example, military personnel might be unwilling to take instruction from civilian ministries, or may opt to adopt a narrow interpretation of ambitious and inclusive cybersecurity mandates.

⁵⁷ Thinyane, M., & Christine, D. (2020). Co-production of cyber resilience in Asia and the Pacific. United Nations University. <https://i.unu.edu/media/cs.unu.edu/page/4531/Preliminary-Report.pdf>

⁵⁸ Christine, D. I. (2021, July 19). Improving cybersecurity means understanding how cyberattacks affect both governments and civilians. *The Conversation*. <https://theconversation.com/improving-cybersecurity-means-understanding-how-cyberattacks-affect-both-governments-and-civilians-163261>

⁵⁹ Thinyane, M., & Christine, D. (2020). Co-production of cyber resilience in Asia and the Pacific. United Nations University. <https://i.unu.edu/media/cs.unu.edu/page/4531/Preliminary-Report.pdf>

Hesitations to address gendered cybersecurity threats through NCS are also based on concerns regarding the 'securitization' of women's digital rights. Such strategies are often developed by national security institutions that do not have enough expertise on gender-related issues, or whose staff and structures might be influenced by gender stereotypes and misogyny, which risks the production of inadequate or even harmful gender mainstreaming strategies. Government actors responsible for the development and implementation of NCS should therefore consider delegating certain tasks related to conceptualizing gender-sensitivity, identifying gendered threats, and monitoring gender mainstreaming metrics to civil society organizations with respective expertise on gender and women's rights. This also necessitates the allocation of adequate resources and accountability mechanisms.

4.2 Integration of Cybersecurity into the NAPs on WPS

4.2.1 Cybersecurity in the Development of NAPs on WPS

The presence of discussions on cybersecurity in NAPs on WPS and the NAP development process was assessed in discussion with women and youth peacebuilders, and centres their expertise in the development of NAPs - from lead authors of NAPs to those who had participated in civil society consultations. Nearly all peacebuilders interviewed identified a connection between cybersecurity and WPS. Women peacebuilders who are involved in the creation of NAPs on WPS for their respective countries shared that cybersecurity did not emerge in conversations and consultations around the NAP. They did note, however, that concerns around technology and digital safety are increasingly present in such spaces. Most peacebuilders interviewed believed that cybersecurity should be included in future NAPs on WPS. They expressed a sense of urgency in addressing cybersecurity concerns in all WPS-related activities, since much of human life – and, by association, peacebuilding work – is connected to digital spaces.

In contrast, most women peacebuilders had not heard of or were not familiar with their country's national cybersecurity strategies. One interviewee noted that in preparation for the interview, she had attempted to obtain a copy of the strategy from the government agency responsible for its creation, with little success. In another discussion a woman peacebuilder shared that their country's current gender-sensitive NCS may be reflective of the positive impact of the participation of gender and women experts in its creation. She emphasized, however, that a gender-sensitive strategy may not necessarily translate into gender sensitivity in practice.

4.2.2 Toward More Cyber-Sensitive NAPs

Women peacebuilders shared several possible approaches to better integrate cybersecurity into NAPs on WPS. The overarching recommendation is to employ a concurrent top-down and bottom-up approach, engaging both high-level experts and actors in the cybersecurity space, and women at the grassroots. At the highest level, agencies or ministries responsible for creating NAPs on WPS should engage the cybersecurity or technology arms of the government, with the goal of coordination and ongoing communication. One interviewee noted that ministries responsible for implementing the NAP, such as ministries of defence or internal affairs, are often engaged in cybersecurity policy and programming. In such cases, existing relationships

The overarching recommendation is to employ a concurrent top-down and bottom-up approach, engaging both high-level experts and actors in the cybersecurity space, and women at the grassroots.

between different government bodies can be used to foster new areas of collaboration focused on cybersecurity.

Focusing on the NAP creation process, most women peacebuilders emphasized a need for the inclusion of cybersecurity experts. According to interviewees, it is most strategic to take advantage of existing expertise in cybersecurity. Bringing in women experts on cybersecurity is seen as more efficient than attempting to develop cybersecurity expertise within the NAP creation mechanisms. Interviewees also highlighted a need for more consistent inclusion of CSOs who work at the intersection of peacebuilding and technology, who are often excluded from NAP creation processes and are not seen as relevant by 'traditional WPS actors'.

In conjunction, a bottom-up approach focuses on the needs and capacities of women and girls at the grassroots. Interviewees noted that cybersecurity issue areas should be integrated into needs assessments conducted prior to drafting a NAP. Awareness-raising around cybersecurity and relevant national policies is another critical step, which will allow those at the grassroots to link their lived experiences and needs to issue areas within cybersecurity. Several interviewees emphasized a need to increase the awareness of community and women leaders on cybersecurity as a tool for strengthening broader awareness-raising at the grassroots level.

When discussing the content of the NAPs on WPS, the peacebuilders interviewed discussed two levels of integration. First, NAPs should be transformed and updated to capture conceptions of security that are not limited in scope to the state or military security sector. From a WPS perspective, NAPs should recognize the significant role of digital spaces for women and girls' participation in political and public life. Persistent insecurity in cyberspace hinders the success of the participation pillar of WPS.

Second, the conceptual recognition of cybersecurity in NAPs on WPS should be supplemented with specific targets, activities, and indicators. Recommendations for this step include activities and indicators focused on education and capacity-building around the use of technology and understanding cybersecurity for women at the grassroots, the creation and implementation of policies related to cybercrime and the protection of privacy, and in particular online GBV. The element of training and education is especially important, as many women, including peacebuilders, only begin to learn about cybersecurity after they experience a cyber threat or attack. Several interviewees discussed the role of localization and engaging local governments in identifying local cybersecurity needs, and better implementing cyber-sensitive NAPs. Given the multi-year implementation window of NAPs, interviewees also recommended integrating a degree of flexibility to allow the implementation of NAPs to keep up with the rapid evolution of technology.

4.2.3 Good Practices from the NAP Development Process

Section 4 of this report outlines the need for inclusive and multi-stakeholder engagement in developing National Cybersecurity Strategies. In many contexts, an inclusive, consultative, and participatory approach to such a national-level strategic document is present and well-established in the NAP development process. The role of civil society, as both co-creators of NAPs on WPS, and a primary actor responsible

for their localization⁶⁰ and implementation, cannot be understated. To better address cybersecurity in WPS NAPs, Member States with strong consultative NAP development processes can draw on this strength to integrate human-level cybersecurity views and needs, particularly those of women and girls, into the NAPs. Member States that retain a centralized or top-down NAP development should consider pathways for increasing the inclusivity of the process, recognizing its benefits as a pathway for forming a gender-sensitive national approach to cybersecurity. The established inclusive and consultative nature of NAP development can serve as a good tool for achieving inclusive and multi-stakeholder engagement with cybersecurity that is absent from most NCS.

4.2.4 Limitations of NAPs as Vehicles for Gender-Sensitive Cybersecurity

Women peacebuilders who were interviewed flagged a major barrier to the integration of cybersecurity into WPS through NAPs. Women-led peacebuilding organizations and women's rights organizations are often occupied with day-to-day needs, and may not have the human and financial resources to consider longer-term issue areas such as cybersecurity. For smaller organizations, the capacity to advocate for the inclusion of cybersecurity issues in WPS discussions is extremely limited. In response to this concern, interviewees raised a need for donors of CSOs to consider the resources needed for organizations to access and use technology, and by extension, participate in advocacy on the topics of technology and cybersecurity – and be willing to allocate funds accordingly. NAPs on WPS should continue to seriously address issues of access to technology and digital devices, connectivity, and digital literacy.

The role of technology in peacebuilding and its relevance to the WPS can no longer be denied. Interviews with women and youth peacebuilders illustrate a gradual translation of this reality to WPS discourse – and NAPs on WPS. Even if cybersecurity is not yet a common part of the discussion, there is potential for its emergence in discussions held by WPS stakeholders in the near future. Since many NAPs on WPS do have established consultative processes, they are an excellent avenue to consult women-led organizations and CSOs on cybersecurity issues, with the goal of creating gender-sensitive approaches to cybersecurity that reflect the needs and priorities of women and girls on the ground. Conversely, the integration of cybersecurity into NAPs on WPS will keep the WPS agenda at pace with the reality of life, and peacebuilding, in a digital age.

It is important also to recognize the limitations faced by the NAP on WPS in engaging with cybersecurity, so long as WPS is considered a “soft security issue” – as opposed to “hard security issues” – which include existing state-centric cybersecurity approaches. There exists a disconnect between the government officials and committees who implement the NAP on WPS and those who are in security-oriented governmental bodies. Such security bodies are more connected to the government officials or bodies responsible for the implementation of the NCS than those who implement the NAP on WPS. As a result, governmental and non-governmental actors connected to the NAP on WPS are shut off from spaces that seriously consider and discuss cybersecurity.

⁶⁰ For more on localization of the WPS, refer to GNWP's Full-Cycle Implementation of Women, Peace and Security, and Implementation through Localization: <https://gnwp.org/what-we-do/global-policy-local-action/implementation-through-localization/>.

5. CYBERSECURITY IN CONFLICT-AFFECTED CONTEXTS

5.1 Cyber Vulnerabilities Unique to Fragile Settings

In conflict-affected contexts, gender inequality and women's and other marginalized groups' rights are deprioritized in national (security) policymaking, or face a lack of implementation due to weak state institutions. This is reflected in, and aggravated by, threats in cyberspace. Women are on the one side faced with gendered cyberviolence, confronted with recruitment efforts of conflict parties, and are more vulnerable to cybercrime. On the other side, in contexts where violence or the potential outbreak of violence is already normalized, the risk of online violence and disinformation escalating into violent attacks and sexual violence in the offline world increases greatly.

Providing adequate security in cyberspace and addressing the fast-changing landscape of cyber threats is still a challenge for many states. This is even more so in fragile and conflict-affected contexts where state institutions are generally weak and lack the human and financial resources to develop, implement and monitor cybersecurity policies. In conflict-affected contexts, citizens might also face additional cybersecurity threats due to inadequate security provisions by technology companies. This is often due to lacking willingness of these actors to spend additional resources to address context-specific cybersecurity needs if a specific country is not lucrative enough from a sales markets perspective, or because they are not held accountable for non-compliance with cybersecurity standards and human rights, due to weak state institutions or limited civil society advocacy capacity. In these contexts, technology companies are often reluctant to invest in cybersecurity provisions and pay less attention to the digital rights compliance of their devices. In the past, they have also shown an unwillingness to invest in human resources to make social media services and online platforms safer by hiring staff with local language skills to improve online content moderation.⁶¹

While international actors can step in to make up for weak state institutions in conflict-affected and fragile contexts to some extent and offer relief and recovery from cyber threats, these efforts often focus on large-scale cyber threats and on providing support to large entities, thus neglecting gendered cyber threats and the cybersecurity needs on the individual level, and cyber harms affecting citizens and civil society organizations.

5.2 The Impact of Cyber Threats on Peacebuilding

The very nature of peacebuilding necessitates trust-building, both within and between communities. Across all countries and regions, women and youth peacebuilders interviewed as part of this research emphasized that threats emerging from cyberspace, particularly online GBV and misinformation and disinformation, are the prime contributor to the loss of trust in peacebuilders and the delegitimization

⁶¹ Hofstetter, J.-S. (2021). Digital Technologies, Peacebuilding and Civil Society. Addressing Digital Conflict Drivers and Moving the Digital Peacebuilding Forward. Institute for Development and Peace. https://www.uni-due.de/imperia/md/content/inef/ir114_hofstetter_final_web.pdf

of their work. In contrast to other activists or human rights defenders, who may work to defend the rights of one group from other groups that violate or oppress, peacebuilders must maintain concurrent relationships and collaborate with groups and factions that are opposed or in conflict with one another. This unique positioning amplifies the impact of cyber threats on peacebuilders, particularly women peacebuilders, who experience the different and gendered dimensions of cyber insecurity discussed in earlier sections of this report. For example, misinformation and disinformation circulating in digital spaces often portray women peacebuilders as collaborators with one party to the conflict, or an armed group, which creates backlash from other communities. As a result, a significant portion of peacebuilders' organizational resources and efforts must be concentrated on identifying and combating misinformation and disinformation, and away from other peacebuilding work. This prevents peacebuilders from focusing their work on higher-level advocacy, in more formal spaces or peace discussions - from which women peacebuilders are already excluded due to their gender.

A women's network has a toll-free number to report cases of online GBV, which was originally created to support women journalists.

Cyber threats also directly affect priority areas of work for peacebuilders. For example, misinformation and disinformation affect post-conflict processes and the re-integration of those affected by conflict into civilian life and communities. In one case shared by a woman peacebuilder, online misinformation portrayed women rescued from militant groups as sex workers who had been providing services to group members. As a result, home communities were unwilling to re-accept these women and girls. In another case, an expert interviewee discussed the impact of misinformation and disinformation on the peace process and referendum. Thus, threats emerging from cyberspace erode the ability of peacebuilders to address critical issues as part of their peacebuilding.

Peacebuilders, including women and youth peacebuilders, also act as providers of cybersecurity in cases where the state is unable to. For example, specific resources for women who have experienced online GBV remain limited and inaccessible. However, women peacebuilders whose activity focuses on ICTs and digital technologies, address this gap by providing support resources at the grassroots level, such as support for reporting online GBV and navigating laws and judicial systems. Online communities of women and activists can provide mutual support, especially when specialized services are absent. One expert shared that some civil society organizations have been mapping online GBV against women peacebuilders and women activists. Some organizations have more robust and well-established tools to engage with online GBV. For example, a women's network has a toll-free number to report cases of online GBV, which was originally created to support women journalists.

In the words of one woman peacebuilder, cyber threats are "part of the reality of war now", and by extension, part of the reality of peacebuilding. Thus, a lack of engagement with cybersecurity, and the specific cyber threats to women peacebuilders and their work, may pose an existential threat to peacebuilding.

6. RECOMMENDATIONS

Improve advocacy and governance by setting strategic priorities.

- 1. Expand the definition of cybersecurity to include a human-centric approach that stresses a human rights perspective.**

- 1.1 Ensure that the human-centric approach to cybersecurity emphasizes the needs of citizens and users, and is complementary to addressing the cyber threats posed to state institutions and corporations.
- 1.2 Employ an inclusive approach to the design and implementation of cybersecurity policies, which stresses the role of civil society actors as recipients of, and contributors to, cybersecurity.
- 2. Raise the profile of gender issues by including a pledge to mainstream gender in national cybersecurity.**
 - 2.1 Include and improve gender mainstreaming in all phases of national cybersecurity strategy development and implementation, considering especially cybersecurity threats that disproportionately affect women and women's rights organizations.
 - 2.2 Improve the meaningful inclusion of all genders in government bodies involved in conceptualizing, researching, designing, governing, implementing and monitoring cybersecurity policies.
- 3. Emphasize a 'do no harm' approach to cybersecurity proliferation to prevent unintended negative consequences of cybersecurity state interventions.**
 - 3.1 Ensure a context-specific approach to the development and implementation of cybersecurity measures by conducting a 'do no harm' assessment at local and national levels.⁶²
 - 3.2 Consider the potential risks of adopting a militarized view on cybersecurity, employing a gender-sensitive approach to risk analysis.
- 4. Improve advocacy on human-centric and gender-sensitive approaches to cybersecurity at national and international levels.**
 - 4.1 In collaboration with UN bodies and advocacy groups, create and support spaces for continued conversations on cybersecurity, gender and peacebuilding, and support women peacebuilders and women's rights organizations' ability to collectively advocate for issues related to cybersecurity.
 - 4.2 Support and promote coalition-building among organizations active in the fields of WPS, technology, and cybersecurity, to improve collaboration and mutual learning.

Improve stakeholder engagement through better cooperation, coordination, and inclusivity.

- 5. Employ a multistakeholder, inclusive, and participatory approach in the creation of national cybersecurity strategies.**
 - 5.1 Facilitate an open and participatory process with contributions from a society-wide spectrum of stakeholders, including activists, academia, and advocacy groups like women's rights groups, and organizations representing other marginalized groups, and possibly also individual citizens.
 - 5.2 Draw on existing networks of women-led organizations, including women's rights organizations and women peacebuilders, to establish a consultative process when discussing cybersecurity and developing relevant policies and frameworks.

⁶² For example, in the justice sector, this could entail emphasizing a survivor-centered approach; in the context of data collection, this should ensure a data-minimization approach; in the context of balancing national security interests, this should entail a risk-averse approach, prioritizing preventing potential risks and human rights violations of citizens over cyber capacity-building.

- 6. Determine cybersecurity needs as part of the NAP creation process.**
 - 6.1 Including cybersecurity in needs assessments conducted to inform the NAP and identify cybersecurity-related needs that can be addressed directly through NAPs on WPS.
 - 6.2 Consider varying access and interaction with technology when determining cybersecurity needs to be addressed by NAPs on WPS, particularly for conflict-affected or insecure regions, contested border areas, and regions with large IDP or refugee populations.
- 7. Align and coordinate cybersecurity-related work across government agencies and departments.**
 - 7.1 Improve cooperation and coordination among government entities in charge of cybersecurity and consult government bodies with specialized expertise on gender equality and digital human rights.
 - 7.2 Connect government ministries and agencies responsible for the creation of the national cybersecurity strategy and the NAP on WPS.
 - 7.3 Align the work of cyber-related departments with the NAP on WPS by creating departmental implementation plans that include specific objectives and indicators for integrating a WPS perspective into their activities and responsibilities.
- 8. Maintain a multi-stakeholder accountability mechanism** to improve oversight and accountability, convene stakeholders in an ongoing manner to review and update national legal and regulatory frameworks, and oversee their implementation.

Improve capacity-building and awareness-raising around cybersecurity and gender, from local to institutional levels.

- 9. Strengthen capacity of actors designing and implementing cybersecurity policies.**
 - 9.1 Provide capacity-building for national cybersecurity and WPS actors to ensure the implementation of a gender-sensitive cybersecurity strategy, strengthen accountability mechanisms, and ensure that national policies are updated on a regular basis to keep pace with the fast-changing cyber threat landscape.
 - 9.2 Provide sensitization and training for all government officials and institutions charged with the design and implementation of cybersecurity policies and laws, on gender- and conflict-sensitive cybersecurity.
 - 9.3 Support capacity-building and awareness-raising among women and girls at the grassroots and local peacebuilders, to better understand, recognize, and respond to threats and risks emerging from cyberspace.
- 10. Improve cybersecurity literacy within the whole of society** by conducting awareness-raising campaigns on gendered cyber threats, providing recommendations on cybersecurity hygiene strategies for women and other vulnerable groups, and providing information on digital rights and channels for reporting cyber incidents, and contact points for legal remedy mechanisms.
- 11. Address cross-sectoral cybersecurity resource inequalities.**
 - 11.1 Consider the specific cybersecurity needs of women's rights organizations and women-led peacebuilding organizations in grant application processes and the provision of funding, when providing funding to grassroots and civil society organizations.
 - 11.2 Identify, support, and fund women-led and civil society organizations working at the intersection of peacebuilding and technology or cybersecurity.

12. Ensure meaningful inclusion of a gender perspective into cybersecurity and technology design beyond the participation level.

- 12.1 Avoid limiting action on improving gender sensitivity in cybersecurity to the tokenistic inclusion of women in the field, including industry and governmental spaces.
- 12.2 Support the development of technologies with reduced gender-bias, and gender-sensitive cybersecurity tools by recognizing and responding to the ways in which the design of technological tools and platforms are inherently gendered, and harm women and girls.

Improve research and knowledge production on the intersections of gender and cybersecurity, and recognize and build expertise.

- 13. **Recognize and draw on grassroots expertise of women and women's rights organizations** and consider the role of citizens as active contributors to the assessment of cyber threats as well as the design and implementation of cybersecurity capacity-building and programming.
- 14. **Commission research** to further analyze and report the gendered dimension of cybersecurity that addresses the gendered impacts of cyber incidents and gendered cybersecurity needs, barriers women and other marginalized groups face in accessing national cybersecurity policymaking processes, legal remedies related to cyber harms, information about their digital human rights, and cybersecurity emergency support.
- 15. **Collect and maintain gender and intersectional disaggregated data** on both the creation and implementation of cybersecurity policies and programs.