System Update: Towards a Women, Peace and Cybersecurity Agenda

LISA SHARLAND | NETTA GOUSSAC | EMILIA CURREY |
GENEVIEVE FEELY | SARAH O'CONNOR

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

www.unidir.org

System Update: Towards a Women, Peace and Cybersecurity Agenda

Acknowledgements

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. The Gender and Disarmament programme is supported by the governments of Canada, Ireland, Norway, Sweden and the United Kingdom. In addition, the authors are grateful to Danielle Cave, Renata H. Dalaqua, Bart Hogeveen, Allison Pytlak, Tom Uren and Kerstin Vignard for their thoughtful comments and suggestions, and the support of the Australian Strategic Policy Institute and its staff. The authors would also like to thank Shimona Mohan for her assistance in preparing this publication.

Notes

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

Citation

Sharland, Lisa et. al. 2021. *System Update: Towards a Women, Peace and Cybersecurity Agenda*. UNIDIR: Geneva. https://doi.org/10.37559/GEN/2021/03

About UNIDIR

UNIDIR is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

About the Gender and Disarmament Programme

The Gender and Disarmament programme seeks to contribute to the strategic goals of achieving gender equality in disarmament forums and effectively applying gender perspectives in disarmament processes. It encompasses original research, outreach activities and resource tools to support disarmament stakeholders in translating gender awareness into practical action.

About the authors

Lisa Sharland is the former Deputy Director, Defence, Strategy and National Security and Head of International Program at the Australian Strategic Policy Institute, and an Adjunct Senior Fellow in the Protecting Civilians in Conflict programme at the Stimson Center in Washington, DC. She has worked on multilateral security issues for over a decade, consulting and undertaking research on women, peace and security, international security, and peacekeeping.

Lisa previously worked as the Defence Policy Adviser at the Permanent Mission of Australia to the United Nations in New York, where she provided advice on peacekeeping and defence-related policy issues and represented Australia in multilateral negotiations in the Security Council and General Assembly.

Netta Goussac is an Associate Senior Researcher within the Stockholm International Peace Research Institute's Armament and Disarmament areas, and a Special Counsel with Lexbridge. Netta has worked as an international lawyer for over a decade, including for the International Committee of the Red Cross and the Australian Government's Office of International Law, and as a lecturer at the Australian National University.

Netta has particular expertise in legal frameworks related to the development, acquisition and transfer of weapons. She has provided legal and policy advice related to new technologies of warfare, including autonomous weapons, military applications of artificial intelligence, and cyber and space security. Since 2017, Netta has participated in the Group of Governmental Experts on lethal autonomous weapon systems. From 2010 to 2013, she participated in the negotiation of the Arms Trade Treaty, and subsequently worked to promote universal adherence to its standards.

Emilia Currey was a researcher with the Australian Strategic Policy Institute's International Cyber Policy Centre. Emilia holds a Bachelor of Laws (Hons.) from the Australian National University. Her research interests include international humanitarian law, foreign interference, gender and human rights issues.

Genevieve Feely was a researcher for the International Program at the Australian Strategic Policy Institute. Her current research interests include the United Nations, multilateralism, peacekeeping, and the women, peace and security agenda. Prior to working at the Australian Strategic Policy Institute, Genevieve was the Fourth Committee intern at the Permanent Mission of Australia to the United Nations in New York, working on a wide range of peace and security issues including peacekeeping and decolonization. She also is a lawyer, admitted to the Supreme Court of Queensland.

Sarah O'Connor was a researcher with the Australian Strategic Policy Institute's International Cyber Policy Centre. She recently joined the 3A Institute as part of the 2021 Master of Applied Cybernetics cohort. Sarah holds a Bachelor of International Relations (Hons.) and Master of Laws (International Law) from the Australian National University. Her research interests include international law, cybersecurity, and the future of warfare and technology.

Table of Contents

List of Acronyms and Abbreviations

AI	Artificial intelligence
GGE	Groups of Governmental Experts
ICT	Information and communications technology
ISIS	Islamic State in Iraq and the Levant
NAP	National Action Plan
OEWG	Open Ended Working Group
RAP	Regional Action Plan
WPS	Women, Peace And Security

Executive summary

As the Women, Peace and Security (WPS) agenda enters its third decade, it is crucial to ensure it is fit to address new and emerging security issues, such as cyberthreats and their gendered implications. To do so requires a shift in focus, moving beyond traditional conflict to encompass other settings where violence against women occurs, including cyberspace.

The accessibility and unattributable nature of cyberspace has exposed women to a disproportionate amount of stalking and online harassment, as well as to targeted disinformation campaigns to dissuade their political participation. This has become even more pronounced in the face of the COVID-19 pandemic, as the world took a digital turn and saw an increase in online violence, misogyny and hate speech directed at women.

The relationship between cyber-enabled threats and cybersecurity has not been comprehensively explored as part of the development of the normative agenda on WPS. Advancing cybersecurity using the WPS agenda can ensure a gender-inclusive cyberspace that protects the rights of women and girls, and that lessons learned from traditional peace and security processes are incorporated for the benefit of a sustainable open, free and stable digital world. Furthermore, examination of cyberspace through the lens of the WPS agenda demonstrates that these incidents are inherently linked to international peace and security.

This paper provides further examination of cyber-related issues affecting the goals of the WPS agenda. It identifies six priority areas that need to be addressed to narrow the gap between WPS and cybersecurity, namely:

» women's participation in cybersecurity negotiations;

» cyberviolence against women and girls;

» online harassment and women's participation in political processes;

» gender and online radicalization;

» gendered impacts of cyber incidents; and

» gender bias in digital technologies.

Bringing these considerations to the forefront of the WPS agenda will provide a much needed 'system update' and ensure that the international community is equipped to deal with twenty-first century international security challenges and their gendered implications.

Main recommendations

To tackle these challenges, the paper recommends an integrated approach that simultaneously advances the WPS agenda and initiatives related to international cybersecurity.

Setting the agenda at the international level

» Develop initiatives to increase the meaningful participation of women in cybersecurity negotiations and to understand the barriers to their participation in multilateral and multi-stakeholder cybersecurity processes.

- Integrate gender considerations into national statements and language proposals as part of United Nations and multi-stakeholder engagement processes focused on international cybersecurity and digital technologies.
- Establish 'cybersecurity' as a theme of a forthcoming debate under the agenda item of 'women and peace and security' in the Security Council.
- Systematically address cybersecurity, including the gendered aspects and impacts of cyber incidents, as part of the Secretary-General's annual report on WPS.
- Ensure that multi-stakeholder dialogues, involving States, civil society as well as technology platforms and social media companies, consider gender dynamics when proposing solutions to restrict the spread of terrorist content and disinformation online.

Policy development at the national level

- Ensure that national cybersecurity policies and activities by governments incorporate diverse gender perspectives as part of their development and implementation across government.
- Develop and/or strengthen gender-inclusive cybersecurity laws, policies and practices that respect the rights of women and girls and that are able to identify and respond to their cybersecurity needs.
- Protect the digital space for women and girls' civic engagement, as well as to prevent cyberviolence against women and girls.
- Increase awareness about what constitutes cyber abuse by developing public campaigns around this issue.

- Adopt laws that criminalize cyber harassment and cyberstalking and address other institutional needs, like public review mechanisms, and implement training within justice and police systems to better investigate and prosecute such crimes.
- Incorporate different dimensions of cybersecurity into the development and review of national action plans on WPS (including those developed at regional and local levels).

Capacity-building initiatives

- Integrate gender perspectives into the development of cyber capacity-building initiatives, materials, and training programmes.
- Ensure that women have equal access to digital technologies.
- Engage women and girls as content creators and developers.

Further research

- Collect gender-disaggregated data on access to and use of digital technologies, and on the impacts of cyber incidents and attacks on different communities, to inform further research and analysis.
- Develop case studies and identify best practices to guide States, international organizations and the private sector to better integrate approaches to WPS and international cybersecurity.

These recommendations will have relevance to governments, policymakers, the private sector, and civil society organizations. The recommendations have application to the development of national and regional policies, as well as approaches by States in the General Assembly's First Committee and the Security Council. Combined they can forge a stronger WPS agenda.

1. Introduction

The WPS agenda provides a useful framework for addressing international security threats and their gendered dimensions, as well as for promoting women's participation in international security decision-making. Thus far, however, the WPS framework has not been systematically applied to cyberspace.

This is not surprising, given that the foundations of the WPS agenda were established in 2000, through Security Council resolution 1325 (2000) on Women, Peace and Security.[1] At that political moment, particular attention was placed in traditional forms of conflict, as the world was still reeling from the Rwandan genocide and the wars in the Democratic Republic of the Congo, Liberia, Sierra Leone and the former Yugoslavia.[2]

That initial resolution in 2000 has so far been followed by additional nine additional WPS resolutions, which collectively form the basis for what is often referred to as the WPS agenda.[3] These resolutions have established areas of reform under 'four pillars', namely, the participation of women in peace and security affairs, inclusion of women in conflict prevention efforts, protection of women and their rights, and addressing women's needs during the relief and recovery phases of conflict. It also urges the United Nations and other actors to integrate a gender perspective into their peace and security efforts. Yet none of the WPS resolutions contain references to 'cyber', 'online', 'technology', 'digital' or 'internet', nor to cyberspace or cybersecurity.

Twenty years after that landmark resolution, the digital world underpins almost every structure and system of modern life. As the WPS agenda enters its third decade, a growing number of national and international actors have been calling for a better integration with cybersecurity issues. During the meetings of the Open-ended Working Group on Developments in the field of information and telecommunications in the context of international security (hereafter, OEWG), between 2019 and 2021, a number of States called attention to gendered dimensions of the cyberspace, including potential gendered impacts of information and communications technology (ICT) incidents, as well as the global gender gap in access to and use of the Internet. The need to strengthen linkages between ICT security discussions and the WPS agenda was also explicitly mentioned in those discussions.[4]

This paper seeks to contribute to these efforts by examining how the WPS agenda can be applied to discussions on international security in cyberspace with the aim of better integrating gender considerations, strengthening gender equality, and transforming our approach to international peace and security with the evolving threats and opportunities posed by cyberspace.

The analysis presented is anchored on a gendered understanding of cybersecurity threat, which recognizes that those 'traditional' ICT incidents, such as denial of service attacks on public services, have gendered outcomes. It also recognizes that doxing, cyberstalking and the non-consensual dissemination of intimate images (i.e. 'revenge porn') are also threats that can arise from the intrusion into or disruption of personal devices and networks,[5] or the malicious use of digital technologies.

This understanding of cybersecurity represents a departure from a common view that considers threats to women's security or gender-based

violence as 'cybersafety' issue and therefore excludes such from discussions around cybersecurity.[6] Rather than siloing the concepts of 'cybersecurity' and 'cybersafety',[7] this understanding seeks to look at them holistically, and acknowledges that "cyber technology has brought new elasticity to concepts of threats to international peace and security".[8] This approach includes a focus on protecting human rights, which is integral to improving women's participation and protection in the online and offline environments.

Drawing on a growing body of research on gender and cybersecurity, as well as desktop research and interviews with representatives of States (see Annex for methodology), this paper articulates the linkages between WPS priority themes—gender equality, women's participation in international security, prevention and protection of violence against women, gender-differentiated needs—and international cybersecurity.

The research starts by situating these distinct discussions within multilateral processes, assessing the extent to which cyber-related issues and WPS have been considered together in negotiations and debates in the General Assembly's First Committee and the Security Council. It then identifies some of the key challenges as they relate to cyberspace and international peace and security, as viewed through the lens of the WPS agenda: women's participation in cybersecurity negotiations, women's participation in political processes, online abuse and violence against women, gender and online radicalization, gendered impacts of cyber incidents, and gender bias in digital technologies.[9] Finally, it presents concrete recommendations for addressing cybersecurity as "the next frontier for the WPS agenda".[10]

By bringing digital technologies and cybersecurity considerations to the forefront of the WPS agenda, this paper seeks to provide a much needed 'system update' and to ensure that the international community is equipped to deal with twenty-first century international security challenges and their gendered implications.

Terminology

Artificial intelligence refers to computer technologies that seek to mimic human or animal cognitive and reasoning capacities, so as to make 'intelligent' machines. Intelligence measures a system's ability to determine the best course of action to achieve its goals in a wide range of environments, though the standard for machines being considered 'intelligent' is constantly moving.[11]

Cybersecurity refers to the processes or practices to protect systems, networks, and other ICTs from malicious attacks, as well as to prevent their misuse, abuse, or manipulation to cause harm to people.

Cyberspace refers to both the Internet and ICTs that connect, use and rely on the Internet such as computers, smartphones, and other Internet-enabled devices.[12]

Gender refers to the roles, behaviours, activities, and attributes that a given society at a given time considers appropriate or as a 'norm' for women and men and girls and boys, as well as non-binary or gender-fluid persons.

Gender norms are socially constructed differences—as opposed to biological differences (sex)—and they function as social rules of behaviour, setting out what is desirable and possible to do as a male or female in a given context.[13]

Gender analysis is a critical examination of how differences in gender roles, activities, needs, opportunities and rights/entitlements affect men, women, girls, boys, non-binary or gender-fluid persons in certain situation or contexts. Gender analysis examines the relationships between genders and their access to and control of resources and the constraints they face relative to each other.[14]

Information and communication technologies (ICTs) refer to programmes, networks and devices that create, store, and transmit data electronically.

Security Council resolution 1325 (2000) on Women, Peace and Security

Security Council resolution 1325 (2000) on women, peace and security reaffirms the important role of women in the prevention and resolution of conflicts, peace negotiations, peacebuilding, peacekeeping, humanitarian response, and post-conflict reconstruction. It stresses the importance of their equal participation and full involvement in all efforts for the maintenance and promotion of peace and security. It urges all actors to increase the participation of women and to incorporate gender perspectives in all United Nations peace and security efforts. It also calls on all parties to conflict to take special measures to protect women and girls from gender-based violence, particularly rape and other forms of sexual abuse, in situations of armed conflict.[15]

2. Situating the WPS agenda and international cybersecurity processes within the United Nations

In order to strengthen the links between WPS and international cybersecurity policy, it is important to understand how these different agendas have evolved and what efforts have already taken place to bridge the gaps. This requires a two-pronged approach. First, understanding the extent to which digital technologies and cybersecurity have been addressed as part of the WPS agenda, particularly within the Security Council and as part of regional, national, and local action plans on WPS. And second, by understanding the efforts—and related constraints—to integrate WPS priority themes and gender equality considerations into multilateral ICT security discussions, particularly in the Groups of Governmental Experts (GGEs) and the OEWG on ICTs and international security.

2.1 To what extent have digital technologies and cybersecurity been addressed as part of the WPS agenda?

The foundations of the WPS agenda were laid out more than two decades ago, with the adoption of the resolution 1325 (2000). This resolution recognized that the impact of conflict on women and women's roles in conflict prevention had long been overlooked. Since then, nine additional resolutions have been adopted on WPS, further developing and expanding this agenda.[16]

The WPS agenda, as framed by the Security Council resolutions, has focused on conflict and post-conflict environments, however feminist scholars and several States have sought to advance the application of the agenda more broadly,[17] despite resistance from some Council members.[18] Central to these arguments has also been the importance of supporting

women's agency and understanding of their own perceptions of security, which have frequently been overlooked in constructing traditional security paradigms,[19] often due to their lack of representation in these security conversations.

Notably, the Security Council has made no reference to cyberspace in the context of WPS over the last two decades.[20] None of the WPS resolutions contain any references to 'cyber', 'online', 'technology', 'digital' or 'Internet', nor to cyberspace or cybersecurity. Looking at the Security Council open debates on WPS, over the past 20 years States or other briefers have linked the agenda, the Internet, or the use of technology in statements on less than two dozen occasions—a relatively small number considering the high rate of State participation in these debates.[21] When there have been indirect references, these have tended to focus on two aspects: the use of ICTs to enable women's rights and their political participation, and the use of ICTs to abuse or perpetrate violence against women.

Early discussions within the Council tended to focus on enabling women's participation in electoral processes and civic life through ICTs. Prior to 2015, a few statements referenced how ICTs were being used to raise awareness about the value of women's participation in political processes, the role of ICTs as a portal to connect women peacemakers, and technology as a capacity-building tool for women campaigning for elections.[22] There were also some references that reflected on the value of digital ICTs in terms of early warning, protecting women and reporting violations.[23] Statements generally focused on some of the opportunities that ICTs presented for enhancing women's political participation and their potential protection from harm.

The focus of statements started to shift from 2015 onwards. While there was still discussion of the opportunities that ICTs provided in terms of

supporting women's participation and their protection, States also started to raise concerns about the risks associated with the harms to women that such platforms facilitated. Some States expressed concerns about the rise in violent extremism and 'new information technologies', the sexual trafficking of women and girls enabled through ICTs, and trolling and online attacks against women journalists.[24] The most comprehensive reference to the potential gendered threats from cyberspace during a WPS debate was made by Kenya in 2017, acknowledging that there was not enough research on "emerging forms and dynamics of cyber-and-technology-led crime, including electronic violence against women, which is becoming more prevalent".[25]

The summary reports from the Security Council's Informal Expert Group on WPS indicates a similar pattern of limited consideration of cybersecurity or ICTs.[26] The only reference to cyberspace, or to the online and digital environment, was during a meeting of the Group on responding to the coronavirus pandemic, in April 2020, which noted that access to digital tools was crucial for women's participation in peace negotiations and ceasefires.[27]

Looking at the annual WPS reports submitted by the Secretary-General to the Council, it is possible to identify references to the opportunities and threats presented in the online and digital environment. For instance, in the 2015 Secretary-General's report on WPS, frequent references were made to the potential of new technologies as powerful tools, in both conflict and non-conflict settings.[28] Since 2015, reports of the Secretary-General have addressed issues relating to the differentiated impact of gender in the online environment to a limited extent, mostly focused on the use of technologies to perpetuate sexual exploitation and violence.[29]

The 2020 Secretary-General's report on WPS recognized the importance of digital inclusion to address gender gaps in access to technology and power, particularly in the context of peace processes.[30] It also acknowledged that women leaders "face harassment, threats and abuse, both in society and online".[31] The report also included discussion of the links between the disarmament agenda and WPS, acknowledging that they have not been fully explored, and women remain underrepresented in multilateral meetings on disarmament.[32] However, none of these reports directly referenced 'cyberspace', 'cybersecurity' or 'ICT-security'. Further discussion or analysis of the nexus between ICTs and WPS through the Secretary-General's report may promote greater diffusion of the issue in statements to Council, which would have a norm-building effect.

Beyond the Security Council, one of the vehicles for the implementation of the WPS agenda have been 'National Action Plans' (NAPs) and 'Regional Action Plans' (RAPs). At the time of writing, 98 countries had adopted NAPs and 11 RAPs had been put in place. Review of these documents also reveals the limited extent to which cyber issues have been integrated into the WPS agenda. Only two NAPs mention cyber threats—the 2019 NAPs of Ireland and of Namibia.[33]

The 2019 Namibian NAP (2019) notes the need "to confront emerging issues … such as … cyber security] and otherwise recognizes two specific types of harms threatened by the cyber domain—cybercrime and cyber-based, gender-based crime.[34] The 2019 Irish NAP (2019) also notes that these are new challenges for international peace and security and calls on the Irish government to support bridging the gender gap in cybersecurity employment. It is the only direct-action item in any NAP to tackle issues of participation in this space.[35]

2.2. To what extent have WPS priorities been addressed in international cybersecurity discussions?

Since 1998, when the Russian Federation tabled a resolution on ICTs in the context of international security, the General Assembly's First Committee has worked on issues related to cybersecurity.[36] The addition of this topic to the First Committee's agenda was initially met with disagreements and scepticism on the part of some States.[37] They disagreed on key concepts of information security (e.g. whether information itself is a weapon), whether new international standards were needed, and the role of the First Committee in international information security discussions.[38] Despite this initial scepticism, the First Committee has emerged as a key player in cybersecurity discussions.

In 2003, the First Committee approved the establishment of a GGE to examine relevant international concepts aimed at strengthening the security of global ICT systems.[39] The group, consisting of experts from 15 States, met in three sessions over the course of a year. Since then, another five GGEs have been established by the General Assembly to continue to study and to discuss issues such as the applicability of international law in cyberspace, international cooperation, and existing and potential threats.

There are no references to 'women', 'girls' or 'gender' in the three reports that have been adopted by consensus by the GGE in 2010, 2013 and 2015.[40] Although these GGE reports include references to respecting "human rights and fundamental freedoms" and "privacy and freedom of expression", there are no references to the potential harms or abuses of rights emerging from the design and utilization of ICTs. Furthermore, no direct links are drawn to the importance of women's participation in cybersecurity, nor

to the importance of gender analysis to understand how ICT security can contribute to or threaten international peace and security. However, there was some progress in the 2021 GGE, with a reference to gender and narrowing the digital divide.[41]

Through resolution 73/27, the General Assembly established an OEWG in which all Member States are invited to participate.[42] Unlike the GGEs, which have a limited membership and meet behind closed doors, the OEWG was designed as an inclusive and transparent process. During the 2019, 2020 and 2021 meetings of the OEWG, a number of delegations called attention to the potential gendered impacts of ICT incidents, as well as to the global gender gap in access to and use of the Internet.[43] A working paper submitted to the OEWG proposed that gender equality and the meaningful participation of women should be at the centre of international peace and security in cyberspace.[44] New research exploring how gender norms shape specific activities related to cybersecurity was presented in side events and multiple civil society organizations highlighted the importance of gender mainstreaming in cyber policies.[45]

Adopted by consensus in March 2021, the OEWG's final report acknowledged the high level of women's participation in OEWG sessions, as well as the prominence of gender perspectives in its discussions, and underscored the importance of narrowing the "gender digital divide" and of promoting the effective and meaningful participation and leadership of women in decision-making processes. Additionally, the final report proposed that capacity-building efforts should "respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory".[46]

However, the Group was unable to reach consensus on language that described the breadth of the discussions and the range of views presented.[47]

Thus the Chair issued his own summary of discussions, which reflected the breadth of considerations made by States on issues related to gender. For instance, some States stressed the interlinkages between norms, confidence-building, and capacity-building, and underscored the need for gender perspectives to be mainstreamed into norm implementation. Some States called attention to the "gender digital divide" and urged that specific measures be taken at the national and international levels to address gender equality and the meaningful participation of women in international discussions and capacity-building programmes on ICTs and international security, including through the collection of gender-disaggregated data. States expressed appreciation for programmes that have facilitated the participation of women in multilateral ICT-security discussions. Moreover, the need to strengthen linkages between this topic and the WPS agenda was also emphasized.[48]

The language incorporated into the 2021 Final OEWG Report and Chair's Summary demonstrates the most substantive progress within United Nations multilateral processes to date to link the WPS and international cybersecurity agendas, including the need to integrate gender perspectives. However, it was very much a compromise text.[49] Some of the strongest proposed language was not included in the conclusions and recommendations, and it did not urge action. Language included in previous drafts urging action to address the 'gender digital divide', collect gender-disaggregated data, address gender inequality and the meaningful participation of women, and recognizing the need to strengthen linkages between the WPS agenda and multilateral ICT-security discussions, ultimately failed to meet consensus of all States.

By contrast to the General Assembly's First Committee, the Security Council has only recently considered the issue of cyber threats and their

implications for international peace and security on one. Discussions about cyber threats have been the focus of several Arria-formula (informal) meetings of the Council since 2016.[50] Some States have utilized the forum of Arria-formula meetings to draw links between aspects of the WPS agenda and cybersecurity. This has included recognition of the importance of gender parity in interventions and women's participation in cyber capacity-building initiatives,[51] gender-sensitive capacity-building,[52] closing the digital divide to fulfil the Sustainable Development Goals.[53] reflecting on links between WPS and cyberspace,[54] and acknowledging the differentiated impact of cyberattacks on critical infrastructure on women and girls.[55]

The Council hosted its first formal open debate on international peace and security in cyberspace in June 2021 during Estonia's presidency. In that debate, the High Representative for Disarmament Affairs acknowledged that ICT threats have a gendered impact and that this was why both women and men needed to participate in "decision-making in the digital arena".[56] However there was limited discussion among States about the different gendered dimensions of cybersecurity. The links between cybersecurity and WPS have not yet matured in the Council's consideration of items on its agenda.

3. System update: Key areas for action

In order to narrow the gap between WPS and cybersecurity, this report identifies six challenges that need to be addressed. Bringing these considerations to the forefront of the WPS agenda and international cybersecurity discussions will provide a much needed 'system update' and ensure that the international community is equipped to deal with twenty-first century international security challenges.

3.1 Women's participation in cybersecurity negotiations

The WPS agenda seeks to achieve the effective and meaningful participation of women across the whole spectrum of international security. Several States and multilateral stakeholders have recognized the importance of achieving this goal in international negotiations and decision-making on cyber issues as well.[57] In interviews conducted for this project, women's participation was frequently mentioned as the most readily identifiable issue in terms of integrating gender into cybersecurity. Respondents emphasized this aspect as matter of gender equality and human rights, as well as a diversity factor that could bring benefits to the discussions and negotiations.[58]

However, women remain underrepresented in multilateral cybersecurity negotiations, comprising, on average, a third of the delegates accredited to the First Committee.[59] This in stark contrast with the Third Committee, dealing with social, humanitarian, and cultural issues, where nearly 50 per cent of the delegates are women.[60] Even more striking is the gender imbalance in smaller groups and taskforces dealing with international security matters, such as the GGEs on ICTs. On average in the six GGEs, women have represented only 20 per cent of experts nominated by governments.[61] Following a commitment by the Secretary-General

to achieve gender parity in disarmament bodies established under his auspices, the 2019 composition of the GGE included 15 men and 10 women.[62]

In an effort to support women's meaningful participation within multilateral discussions on issues related to ICTs in the context of international security, in 2019 the governments of Australia, Canada, the Netherlands, New Zealand and the United Kingdom established the Women in International Security and Cyberspace Fellowship.[63] As part of the Fellowship, 35 women received sponsorship to attend the OEWG meetings in New York, as well as training from the United Nations Institute for Training and Research on multilateral negotiations.[64] Following the training session of the Fellowship, there was a noticeable increase in the level of women's engagement in the OEWG on ICTs in the Context of International Security, as over 40 per cent of official statements in the second substantive session of were delivered by women.[65]

Furthermore, the final report of the OEWG recognized the importance of women's participation in decision-making processes around ICTs in international security.[66] However, the OEWG report did not go further in urging States to take action to address women's meaningful participation in cybersecurity discussions and capacity-building programmes. This shows that there is scope for further action, engagement and research to understand the barriers to women's participation and to ensure that women are afforded opportunities to meaningfully participate in and influence cybersecurity processes.

Women's participation in international cybersecurity decision-making matters as it can provide one pathway to diminishing gender inequality, providing a diversity of perspectives which can enable more careful information processing and better policy decisions.[67] Importantly, women are in the best position "to identify their unique cybersecurity needs,

and contribute their lived experiences to the knowledge-base, informing cybersecurity".[68] Efforts to increase women's participation also need to be complemented by "actively incorporating gender perspectives into policies and programmes",[69] which supports a more comprehensive approach to advancing WPS as part of cybersecurity.

3.2 Cyber violence against women and girls

Prevention of and protection from all forms of violence that affect women and girls are at the core of the WPS agenda. Digital ICTs have provided women with different tools to mobilize and to engage with online applications that share information about threats to their security. For instance, there are examples of women utilizing digital technologies to share information and map security concerns to enhance their protection and to provide support to early-warning mechanisms in conflict-affected areas.

However, the online environment has also exposed women to a disproportionate level of violence and abuse in digital spaces. Women of all kinds, from politicians, to human rights defenders, to private users, face online harassment and threats, which in some instances has led to attacks on their physical safety. Therefore, protecting women and girls from cyberviolence must be part of the WPS agenda as well.[70]

In some cases, targeted attacks and campaigns of harassment, particularly on social media, are used to silence women in public spaces and communities.[71] At times, online harassment mutates into armed violence, such as in the case of online radicalization of 'incels'. "Otherwise known as 'involuntarily celibates', incels are part of a virulently misogynist, racist and male-supremacist subculture that manifests most visibly online.

Nonetheless, self-proclaimed incels have committed acts of violence, mostly shootings."[72]

Online spaces and the dark web may be utilized to perpetuate violence against women, including through crimes such as human trafficking. Online sexual exploitation and abuse is often accompanied by or can lead to in-person violence against women and girls.[73] Additionally, lockdowns and travel restrictions imposed by the COVID-19 pandemic have resulted in a spike in the online sexual exploitation and abuse of women and girls, including commercial sexual exploitation and an increase in people attempting to access illegal websites featuring child sexual abuse material.[74]

To grasp the many forms of cyberviolence against women and girls, the Violence Against Women learning network identified six broad categories (See Table 1).

Table 1. Cyberviolence Against Women and Girls[75]

Hacking	The use of technology to gain illegal or unauthorized access to systems or resources for the purpose of acquiring personal information, altering or modifying information, or slandering and insulting the victim and/or their representative organizations.
Impersonation	The use of technology to assume the identity of the victim or someone else in order to access private information, embarrass or shame the victim, contact the victim, or create fraudulent identity documents.

Surveillance / Tracking	The use of technology to stalk and monitor a victim's activities and behaviours either in real-time or historically.
Harassment	The use of technology to continuously contact, annoy, threaten, and/or scare the victim. This is ongoing behaviour and not one isolated incident.
Recruitment	The use of technology to lure potential victims into violent situations.
Malicious Distribution	The use of technology to manipulate and distribute defamatory and illegal materials related to the victim and/or women's organizations.

Violence online and offline feed into each other. Protecting women and girls from cyberviolence is an integral part of the WPS agenda and should be included in national and regional action plans to implement resolution 1325 (2000). This will require States to adjust how they approach issues that have traditionally been framed as a domestic concern (e.g. human harms of cyber-enabled violence) in WPS national action plans, rather than focusing only on outward facing security threats.[76] Likewise, this issue of cyberviolence should also be addressed in national legislation, as new laws may be needed to update the definition of what constitutes

cyberviolence, to include the different types of cyber-enabled abuse and violence against women and girls.

3.3 Women's participation in political processes

A digital gender gap is evident in most parts of the world, as young men from Western countries are much more likely to have access to the Internet than women from emerging economies.[77] In 2015, the Global Study on the implementation of resolution 1325 (2000) acknowledged that barriers to women's access to technology could limit their empowerment.[78] Such barriers may also restrict their participation in civic life. In view of this, the Secretary-General has called for "digital inclusion initiatives" to address gender gaps and to strengthen mechanisms to "meaningfully engage all constituents".[79]

While ICTs enable opportunities for grass-roots engagement with a wider range of individuals and the formation of online communities, they also facilitate abuse and harassment, by individuals, groups and even State actors. Such abuse online can deter women from participation in political processes, particularly running for political office. The 2019 Secretary-General's Report on Women and Peace and Security, for example, notes that women candidates for elections faced intimidation and harassment online in several countries.[80] Such harassment can act as a barrier to women's participation in politics.[81]

The anonymous nature of the online environment, coupled with the algorithms of social media platforms, can facilitate the rapid spread of misinformation and disinformation. Gendered and sexualized

disinformation campaigns—led by State actors in some instance—can undermine the credibility of women and the success of their political campaigns in these contexts.[82]

One form of gendered disinformation that has been utilized are 'deepfakes'. Deepfakes are digital forgeries (images, video and audio) created through deep learning, a subset of artificial intelligence (AI).[83] Deepfakes replicate the look and sound of real human speech and movement, allowing users to create realistic videos of people doing and saying things they never did or said.[84] They can be used for character assassination and smear campaigns online,[85] and even to silence women human rights defenders through intimidation and fears of sexual and gender-based violence.[86] Deepfake videos circulated online can not only undermine the political participation of women, but also more broadly present a gendered security issue.[87]

Women's participation in politics and in government institutions is central to efforts to strengthen women's representation and to amplify their voices, further advancing efforts to strengthen the WPS agenda. However, the ease with which ICTs allow for women to be intimidated, harassed, and vilified online mean that women will continue to face additional barriers to participation in political processes. While there is still a lack of research on the impact that online intimidation and harassment have on women candidates, it can form a pattern of abuse intended to intimidate women and to prevent them from participating in political life.

3.4 Gender and online radicalization

Terrorist and extremist groups have utilized cyberspace to promote misogynistic narratives to form communities and to radicalize individuals, which threatens international security and the objectives of the WPS

agenda.[88] Some terrorist organizations have been highly effective at applying a gender lens to their recruitment programmes to capitalize on the engagement of men and women. The Islamic State in Iraq and the Levant (ISIS), for example, promotes highly gendered narratives and 'idealized' masculine and feminine roles in their recruitment strategies.[89] As researchers have noted, terrorist groups are "more active and advanced in thinking about gender than the international counter terrorism community".[90]

In the case of recruitment to ISIS, research has found that women were at greater risk of being radicalized and recruited online than offline.[91] This may also have an impact on the extent to which different groups of people are radicalized, depending on their access to the Internet, and power structures in society. Research has also indicated that, once recruited, women's roles largely include sharing propaganda and recruitment material and raising funds online, all of which enables physical violence to be perpetrated by these groups.[92]

The use of the Internet to spread ideology and to radicalize individuals has "exponentially increased the pool of potential audience members" and targets for these extremist organizations.[93] Attacks perpetrated by far-right terrorists in the last few years have been noticeably 'Internet-centric' in that they were planned and streamed online.[94] However, the gendered influences and impacts of far-right extremist rhetoric online remain largely unexplored in the literature and State discussions.[95] Understanding the different appeal of and gendered engagement with these platforms is key to addressing some of the risks they present to peace and security, in order to prevent and to respond to the radicalization of individuals via these platforms.

Restricting the spread of terrorist content remains the responsibility of social media and technology companies, although that role is increasingly being regulated by national laws. Approaches differ between platforms, enabling individuals to pick and choose how they engage. Some social media sites, such as Twitter and Facebook, have taken steps to disable accounts and to remove content when it reaches a threshold of concern, but this is often too late. Even when this does occur, banned communities simply migrate to platforms with less moderation or new accounts are created.[96] There are also concerns that measures to restrict potential terrorist content may also be framed in a manner to restrict human rights and free speech, which may have an impact on women's mobilization and political participation.

Multi-stakeholder dialogue, involving States, civil society, as well as technology platforms and social media companies, is needed to develop effective ways of restricting the spread of terrorist content and disinformation online.[97] Knowledge of gender dynamics is likely to enhance the effectiveness of such initiatives, which have, thus far, been designed in a "gender blind" manner.[98]

3.5 Gendered impacts of cyber incidents

Resolution 1325 (2000) recognizes the gendered impacts of conflict, as well as the differential security needs of women and girls. Much like traditional conflict, the use of ICTs by States or non-State actors can have different impacts on men and women.[99] For instance, women often rely on mobile and online communications to manage their safety. Cutting off the Internet through shutdowns can deprive them of these tools. Additionally,

opportunities for education, economic benefit and personal safety for women may be impacted when Internet shutdowns take place.[100]

Similarly, data breaches can have a disproportionate impact on women. An example presented by Brown and Pytlak (2020) referred to a data breach that occurred in São Paulo, Brazil, in July 2016. It exposed the health records of 650,000 patients, including information about pregnancy and abortion care. Abortion is illegal in certain circumstances in Brazil, meaning women's rights were likely to be impacted differently by the data breach, and potentially expose them to charges.[101] Failing to consider the gender-differentiated impacts of these incidents may mean that such events are not considered as threatening as other cyber incidents.

The ongoing collection of gender-disaggregated data by civil society and researchers when these events take place, including analysis of the way that men, women, non-binary identifying individuals, and different communities are affected can enable more effective policy responses when these events take place, strengthening efforts to support women's relief and recovery following the incident.

More research is required to examine the gender-differentiated impact of cybersecurity policy instruments (such as Internet shutdowns), data breaches and attacks on critical infrastructure. States should also seek to incorporate a gender perspective into the development of their policies around protecting critical infrastructure, including how they frame and define what constitutes 'critical infrastructure' and 'critical information infrastructure', and the priority attached to different types of incidents.

3.6 Gender bias in digital technologies

Technology reflects and, at the same time, shapes the society that creates it. By extension, technology incorporates and, at times, perpetuates gender and other structural inequalities that already exist within a given society. Humans are the first source of bias, directly influencing the input data used to test and to train algorithms. Even largely automated processes rest on human judgments about organizational priorities, allocation of resources and capacity-building—all of which open the potential for the creation or intensification of inequalities.[102] The result is often gendered assumptions built into algorithms and biased data.[103]

Research has showed that threat models, reporting and user-control procedures, and advertising of cybersecurity technologies mean that women are more likely to have cybersecurity threats downplayed or omitted, more likely to have additional security burdens, and more likely to be affected by disingenuous cybersecurity marketing.[104] For example, the design of smart household devices has not adequately included intimate partner violence in the 'threat modelling' phase of design, meaning that supposedly secure smart devices increase gendered risks.[105] To reduce the occurrence of these inadvertently dangerous blind spots, it is thus important that the design and threat-modelling processes include diverse perspectives and people from minoritized groups.[106]

A gender-diverse workforce could be a means of avoiding such blind spots. According to the World Economic Forum's 2018 Global Gender Gap Report, women account for less than a quarter of AI professionals worldwide.[107] This disparity in the workforce has raised concerns about

replicating and reinforcing biases within AI systems, such as "existing gender stereotypes and discriminatory social norms".[108]

There is evidence that some of the algorithms put in place in criminal justice systems may result in disproportionate sentences for women and other minority groups due to predictions about recidivism rates based on biased data.[109] Biases in such algorithms may also present challenges in terms of cybersecurity when it comes to malicious use or system intrusions. Software to prevent the intrusion of malicious actors often relies on algorithms to identify patterns. While it is argued that such processes can augment the ability of humans to identify and respond to threats, it may be flawed if the data it is relying on includes certain assumptions about perpetrators (i.e., that they are men).

Biases in datasets and in the cyber and AI workforces raise questions about the scenarios or situations where AI may be applied within the security domain, in terms of autonomous weapons (that are enabled through online platforms), or decision-making processes and algorithms. The emerging nature of these technological developments means that further research is required to explore these challenges. There is also an outstanding research question as to whether digital technologies that reinforce gender inequalities across society may contribute to the conditions that facilitate conflict within a country or predict State aggression, in the same way that other indicators across society suggest this link.[110]

4. Conclusions: Towards a Women, Peace and Cybersecurity agenda

The digital world underpins every structure and system of modern life. Cyberspace offers opportunities to advance the WPS agenda, but also presents threats to women's empowerment and security. Yet, as demonstrated in this paper, cybersecurity has not been integrated into the consideration of the WPS agenda. It is past time to ensure that the WPS framework is fit to address new and emerging security issues, such as cyber threats and their gendered implications.

There are multiple avenues for bringing these policy areas closer. At the national, regional and multilateral levels, it is important to integrate gender considerations into cybersecurity policies, on one hand, and to include cybersecurity in WPS policies and action plans, on the other. Concretely, this paper has outlined six key areas for doing so and advancing gender equality in cyberspace.

» Women's participation in cybersecurity negotiations

Women remain underrepresented in cybersecurity negotiations and more research is needed to understand the specific barriers preventing their full, equal and meaningful participation. Additionally, action should continue be taken to support diverse women's engagement, such as the Women in Cyber Fellowship. Efforts to increase women's participation also need to be complemented by actively incorporating gender perspectives into policies and programmes.

» Cyberviolence against women and girls

Women of all kinds, from politicians, to human rights defenders, to private users, face online harassment and threats. To tackle this issue, it is important to increase awareness about what constitutes cyberviolence by developing public campaigns. It is also necessary to ensure that national legal systems are equipped to prevent and also to prosecute cases of cyberviolence by enacting legislation that criminalizes acts of cyber harassment and cyberstalking, and by providing training within the justice and police system.

» Online harassment and women's participation in political processes

It is crucial to ensure that women and girls have access to ICTs and are able to use the digital space for civic engagement. Further analysis and research into how such behaviours in cyberspace impact women's meaningful political participation is required, in order to identify ways to address some of these threats.

» Gender and online radicalization

More gender-sensitive research is needed examining the different factors influencing men and women's radicalization, their recruitment, and their

agency in these online environments. Gender-sensitive research is required into the factors that influence radicalization in the online environment. Multi-stakeholder dialogues involving technology platforms and social media companies are needed to discuss effective ways of restricting the spread of terrorist content and disinformation online.

» Gendered impacts of cyber incidents

Further gender-disaggregated data and research is required to understand and to address the range of differentiated impacts of cybersecurity incidents and attacks on civilians. States should also seek to incorporate a gender perspective into the development of their policies aimed at protecting critical infrastructure, including how they frame and define what constitutes 'critical infrastructure' and the priority attached to different types of incidents.

» Gender bias in digital technologies

Ensuring diversity in cyber and AI workforces and processes is one way to address bias in digital technologies. Furthermore, it is important to integrate gender perspectives into the development of cyber and AI capacity-building initiatives, materials, and training programmes.

Bringing these considerations to the forefront of the WPS agenda will provide a much needed 'system update' and ensure that the international community is equipped to deal with twenty-first century international security challenges and their gendered implications.

5. Specific Recommendations

The WPS agenda offers an important framework to conceptualize 'cybersecurity' and to strengthen gender considerations in cybersecurity. Drawing on these lessons, this paper offers the following recommendations for States, the United Nations and civil society organizations to consider as part of their engagement in United Nations processes.

Recommendations to States in the General Assembly

- Integrate gender considerations into national statements and multilateral negotiations on ICTs and cybersecurity.
- Deliver statements and propose language in First Committee resolutions on developments in the field of ICTs in the context of international security and next OEWG that:
  - acknowledge that the design and use of ICTs can affect men, women and other marginalized groups differently, and that gender considerations need to be applied to recognize the impact of ICTs on international peace and security;

  - urge States to continue their ongoing efforts to increase the meaningful participation of women in organizations and intergovernmental processes examining ICTs;
  - recognize the important role of civil society in discussions and negotiations around ICTs in the context of international peace and security; and
  - encourage States to integrate gender considerations into the development of national cybersecurity policies.
- Acknowledge the gender-differentiated impacts of cybersecurity activities in statements, resolutions and reports, including resolutions on women and disarmament in First Committee. In acknowledging the applicability of international legal frameworks to cyberspace activities, States could specifically reference obligations regarding international human rights law, particularly women's rights.

Recommendations to States in the Security Council and its subsidiary bodies

- Convene an Arria-formula meeting focused on a topic examining the linkages between cybersecurity and women, peace and security.
- Establish 'cybersecurity' as a theme of a forthcoming open debate under the agenda item of 'women and peace and security' in the Council.
- Ensure that statements delivered at open debates on WPS recognize the opportunities and threats presented by ICTs and cyberspace to women's participation and protection, and to conflict prevention, and acknowledge the need for gender perspectives to be integrated into efforts to strengthen cybersecurity.

- Request the Secretary-General's annual report on WPS to address cybersecurity, including the gendered aspects and impacts of cyber incidents.
- Utilize the Informal Expert Group on WPS in the Security Council to ask questions about gendered dimensions or the impact on women when there are cyber incidents in country situations under discussion.

Recommendations to States on national and regional policies

- Ensure that national cybersecurity policies and activities by governments incorporate diverse gender perspectives as part of their development and implementation across government.
- Integrate gender perspectives into the development of cyber capacity-building initiatives, materials, and training programmes.
- Ensure multi-stakeholder dialogues, involving States, civil society, as well as technology platforms and social media companies, consider gender dynamics when proposing solutions to restrict the spread of terrorist content and disinformation online.
- Incorporate different dimensions of cybersecurity into the development and review of national action plans on WPS (including those developed at the regional and local levels).
- Commission research and analysis that will:
  - collate gender-disaggregated data and examine the impacts of cyber incidents and attacks on different communities;
  - develop a series of case studies and best-practice approaches to offer guidance to States, international organizations and the private

sector, which might include examination of issues related to how the online environment affects women's political participation, the gendered dimensions of online radicalization, the gender differentiated impacts of cyber incidents, and the role of bias in digital technologies and its potential impacts on gender equality and international peace and security; and

» identify the barriers to women's participation in multilateral and multi-stakeholder cybersecurity processes.

Annex – Interviews and Methodology

This report drew primarily on desktop research of United Nations documents, statements by States and civil society, research reports and academic papers. This research was complemented by interviews with diplomats and members of the GGE from Australia, Canada, Kenya, Malaysia and the Netherlands.

The following terms were used to analyse the 10 WPS resolutions and open Security Council debates on WPS. Justifications have been included below as to why certain terms were chosen.

'Computer'	Included to capture any discussion on devices through which engagement with the cyber domain occurs
'Cyber'	Included as the phrase directly frames this paper
'Information'	Included to capture references to 'information communication technology/technologies'
'Internet'	Included as a common reference for online spaces
'Online'	Included as a common reference for online spaces
'Phone'	Included to capture any discussion in the early years of WPS of then-emerging technologies such as SMS and mobile phone networks
'Technologies'	Included as the phrase directly frames this paper
'Technology'	Included as the phrase directly frames this paper

Endnotes

1. Security Council, UN document S/RES/1325, 31 October 2000, https://undocs.org/S/RES/1325(2000).

2. Henri Myrttinen, "Connecting the Dots: Arms Control, Disarmament and the Women Peace and Security Agenda", UNIDIR, 2020, https://unidir.org/sites/default/files/2020-12/Connecting%20the%20Dots_0.pdf.

3. At the time of writing, these are resolutions 1820 (2009), 1888 (2009), 1889 (2010), 1960 (2011), 2106 (2013), 2122 (2013), 2242 (2015), 2467 (2019), and 2493 (2019).

4. General Assembly, UN document A/AC.290/2021/CRP.3, 10 March 2021, para. 37, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

5. Katharine Millar, James Shires, and Tatiana Tropina, "Gender Approaches to Cybersecurity: Design, Defence and Response", UNIDIR, 2021, https://doi.org/10.37559/GEN/21/01.

6. Julia Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity", *St Antony's International Review* vol. 15, no. 1, 2019, https://ssrn.com/abstract=3429851.

7. For a framing of these concepts, and the need for greater empathy and synergy on these issues among cyber professionals, see Alex Stamos, "Tech's Adversaries vs Enemies", *Medium*, 13 January 2020, https://medium.com/@alexstamos/techs-adversaries-vs-enemies-a5ca09e09aca.

8. Security Council Report, "In Hindsight: The Security Council and Cyber Threats", 23 December 2019, https://www.securitycouncilreport.org/monthly-forecast/2020-01/the-security-council-and-cyber-threats.php.

9. Due to the limitations of this paper, the discussion will focus largely on the experiences of women, with some limited consideration of the experiences of other gender identities.

10. UN-Women, "Women, Peace & (Cyber) Security in Asia and the Pacific", 2020, p. 1, https://asiapacific.unwomen.org/en/digital-library/publications/2020/06/action-brief-women-peace-and-cyber-security-in-asia-and-the-pacific.

11. UNIDIR, "The Weaponization of Increasingly Autonomous Technologies: Artificial Intelligence", *UNIDIR Resources*, no. 8, 2018, p. 2, https://www.unidir.org/files/publications/pdfs/the-weaponization-of-increasingly-autonomous-technologies-artificial-intelligence-en-700.pdf. Definitions contained in the Terminology box have been adapted or quoted from the sources listed in the endnotes.

12. Camino Kavanagh, "The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century", UNIDIR, 2017, p. 7, https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf.

13. UNIDIR, "Gender Perspectives", https://unidir.org/gender-perspective.

14. Renata Hessmann Dalaqua, Kjølv Egeland, and Torbjørn Graff Hugo, "Still Behind the Curve: Gender Balance in Arms Control, Non-Proliferation and Disarmament Diplomacy", UNIDIR, p. 10, https://doi.org/10.37559/WMD/19/gen2.

15. United Nations, 'Landmark resolution on Women, Peace and Security', https://www.un.org/womenwatch/osagi/wps/. See also Security Council, UN document S/RES/1325, 31 October 2000, https://undocs.org/S/RES/1325(2000).

16. At the time of writing, these are resolutions 1820 (2008), 1888 (2009), 1889 (2009), 1960 (2010), 2106 (2013), 2122 (2013), 2242 (2015), 2467 (2019), and 2493 (2019).

17. The Human Rights Council adopted its first resolution on WPS in 2020; see UN Document A/HRC/RES/45/28. Also see Sara E. Davies and Jacqui True (eds), *The Oxford Handbook of Women, Peace and Security*, 2019.

18. Prior to 2019, all WPS resolution had been adopted unanimously, although there were differences expressed in the negotiating processes. In April 2019, resolution 2467 was not adopted unanimously, with China and the Russian Federation abstaining; see Security Council Report, "In Hindsight: Negotiations on Resolution 2467 on Sexual Violence in Conflict", 2 May 2009, https://www.securitycouncilreport.org/whatsinblue/2019/05/in-hindsight-negotiations-on-resolution-2467-on-sexual-violence-in-conflict.php.

19. These institutions tended to focus on so-called 'hard' or 'traditional' security issues which focused on State-on-State behaviours, rather than 'private' or 'domestic' security concerns, such as gender-based violence. See Phoebe Donnelly, 'Sustaining Feminist Curiosity for the Future of Women, Peace and Security: Q&A with Cynthia Enloe', IPI Global Observatory, 6 October 2020, https://theglobalobservatory.org/2020/10/sustaining-feminist-curiosity-for-future-of-wps-qa-with-cynthia-enloe/; and Julia Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity", *St Antony's International Review* vol. 15, no. 1, 2019, https://ssrn.com/abstract=3429851.

20. To assess the consideration of ICTs and cyberspace by the Security Council in the context of WPS, all open debates and resolutions since 2000 on WPS were reviewed and analysed for any linkages to 'cyber', 'technology', 'online' and 'internet' among other related terms; see Annex.

21. The first link appears to have been made by the representative for Bangladesh in 2008, who noted the potential for ICT tools to raise public awareness of 'the strengths of women in promoting peace and security around the world'; see Security Council, UN document S/PV.6005 (Resumption 1), 29 October 2008, p. 10, https://undocs.org/en/S/PV.6005(Resumption1).

22. See, for instance, statement by Bangladesh in 2008 debate on WPS (https://undocs.org/en/S/PV.6005); statement by Australia on 28 October 2011 (https://undocs.org/S/PV.6642, p. 33); and statement by Netherlands on 30 November 2012 (https://undocs.org/en/S/PV.6877, p. 56).

23. See, for instance, statement by United States of America on 18 October 2013 (https://undocs.org/S/PV.7044, p. 12).

24. See, for instance, statement by Belgium on 13 October 2015 (https://undocs.org/en/S/PV.7533, p. 78); statement by France on 28 March 2016 (https://undocs.org/S/PV.7658, p. 26); and statement by the United Arab Emirates (https://undocs.org/S/PV.7704, p. 46); and statement by the European Union on 2 June 2016 (https://undocs.org/S/PV.7704, p. 37). Lithuania noted in the debate on 25 October 2016 that women journalists were subject to trolling and attacks online (https://undocs.org/S/PV.7793, p. 89).

25. See statement by Kenya at Security Council debate on 27 October 2017 (https://undocs.org/S/PV.8079, p. 70).

26. The Informal Expert Group was established by resolution 2422, to better inform and guide the Council's work on WPS. Discussions take place among country-specific and WPS experts from States serving on the Council, on a range of country-specific, situations throughout the year.

27. Security Council, UN document S/2020/439, 28 May 2020, p. 5, https://undocs.org/S/2020/439.

28. Similar themes were picked up in the Global Study on 1325, which included two recommendations on how Member States and civil society could better ensure the positive use of technology to ensure prevention and protection during conflict as well as to bridge 'the digital gender divide'; see UN-Women, *Preventing Conflict, Transforming Justice, Securing the Peace: A Global Study on the Implementation of United Nations Security Council Resolution 1325*, 2015, p. 407, https://reliefweb.int/sites/reliefweb.int/files/resources/UNW-GLOBAL-STUDY-1325-2015.pdf.

29. See, for example, Security Council, UN document S/2015/203, 23 March 2015, p. 25, https://undocs.org/en/S/2015/203.

30. Security Council, UN document S/2020/946, 25 September 2020, p. 6, https://undocs.org/en/S/2020/946.

31. Ibid., p. 20.

32. Ibid., p. 18.

33. These include references to 'cyber related threats' in conflict (Ireland 2019), the impact of 'cyber crime' (Namibia 2019; Kenya 2020) and the threats posed by 'cyber harassment' to women's organizations and human rights defenders (Netherlands 2021). For further data, see Women's International League for Peace and Freedom, National Action Plans at a Glance, http://1325naps.peacewomen.org/ and Hamilton, Caitlin and Laura J. Shepherd (2020) WPS National Action Plans: Content Analysis and Data Visualisation, v2. Online, at https://www.wpsnaps.org/. See also Myrttinen, Henri. 2020. "Connecting the Dots: Arms Control, Disarmament and the Women Peace and Security Agenda". United Nations Institute for Disarmament Research. https://doi.org/10.37559/GEN/20/01

34. Republic of Namibia, "Namibia National Action Plan on Women, Peace and Security: Moving United Nations Security Council Resolution 1325 Forward, 2019–2024", 2019, https://www.peacewomen.org/sites/default/files/Namibia%20NAP%20(2019-2024).pdf.

35. Government of Ireland, "Women, Peace and Security: Ireland's Third National Action Plan for the Implementation of UNSCR 1325 and Related Resolutions 2019–2024", 2019, https://dfa.ie/media/dfa/ourrolepolicies/womenpeaceandsecurity/Third-National-Action-Plan.pdf.

36. General Assembly, UN document A/RES/53/70, 4 January 1999, https://undocs.org/A/RES/53/70.

37. Also see responses by Australia, the United Kingdom, and Sweden (on behalf of the European Union) in General Assembly, UN document A/54/213, 10 August 1999, https://undocs.org/A/54/213; and General Assembly, UN document A/56/164, 3 July 2001, https://undocs.org/a/56/164.

38. Eneken Tikk-Ringas, "Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998–2012", ICT4Peace, 2012, pp. 4–5, https://ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf.

39. General Assembly, UN document A/RES/58/32, 18 December 2003, https://undocs.org/A/RES/58/32.

40. General Assembly, UN document A/65/201, 30 July 2010, https://undocs.org/A/65/201; General Assembly, UN document A/68/98, 24 June 2013, https://undocs.org/A/68/98; and General Assembly, UN document A/70/174, 22 July 2015, https://undocs.org/A/70/174.

41. "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", advance copy, 28 May 2021, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

42. General Assembly, UN document A/RES/73/27, 11 December 2018, https://undocs.org/

en/A/RES/73/27.

43. For detailed information on national statements highlighting the importance of gender mainstreaming in the OEWG process, see Cyber Peace & Security Monitor, vol. 1, no. 7, 2020, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.7.pdf.

44. See "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'", https://www.un.org/disarmament/wp-content/uploads/2019/09/canadian-position-paper-oewg-en.pdf.

45. Deborah Brown and Allison Pytlak, "Why Gender Matters in International Cyber Security", Women's International League for Peace and Freedom and the Association for Progressive Communications, 2020, https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf; and Katharine Millar, James Shires, and Tatiana Tropina, "Gender Approaches to Cybersecurity: Design, Defence and Response", UNIDIR, 2021, https://doi.org/10.37559/GEN/21/01.

46. General Assembly, UN document A/AC.290/2021/CRP.2, 10 March 2021, para. 12, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

47. For instance, the Russian Federation opposed inclusion of some language on women's participation and gender perspectives, arguing this was did not relate to the OWEG's mandate; see Russian amendments to the zero draft of the OEWG as of 19 January 2021, https://front.un-arm.org/wp-content/uploads/2021/02/RF-OEWG-zero-draft-report-with-the-Russian-amendments-ENG.pdf.

48. General Assembly, UN document A/AC.290/2021/CRP.3, 10 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

49. While the Chair's Summary was issued under his own authority, the summary of discussions appeared in all the drafts discussed by States, was commented upon and negotiated up until the final session of the OEWG, when it was determined that consensus would not be reached on the summary of discussions. As the content of the Chair's Summary was negotiated until its removal from the outcome document, it too represents a compromise text.

50. Of the five Arria-formula meetings that have included a focus on cyber-related issues, three have focused specifically on cybersecurity. The first was in November 2016, hosted by Spain and Senegal on the topic of 'Cybersecurity and International Peace and Security'. In May 2020, Estonia hosted the second Arria-formula meeting on cyber issues, entitled 'Cyber Stability, Conflict Prevention and Capacity Building', and in August 2020 Indonesia (in cooperation with

Belgium, Estonia, Vietnam and the ICRC) hosted an Arria-formula meeting on 'Cyber-Attacks Against Critical Infrastructure'. See Security Council Report, "Arria-formula Meeting on Cyber-Attacks against Critical Infrastructure", 25 August 2020, https://www.whatsinblue.org/2020/08/arria-formula-meeting-on-cyber-attacks-against-critical-infrastructure.php.

51. See statements delivered by Australia at Arria-formula Meeting on 'Cyber Stability, Conflict Prevention and Capacity-Building', hosted virtually on 22 May 2020, https://vm.ee/sites/default/files/Estonia_for_UN/unsc_-_cyber_arria_22_may_2020_-_australian_statement_002.pdf, and by Canada, https://vm.ee/sites/default/files/Estonia_for_UN/canada-cyber_statement.pdf.

52. See statement by Ecuador at Arria Formula Meeting on 'Cyber Stability, Conflict Prevention and Capacity-Building' hosted virtually on 22 May 2020, see on 22 May 2020 https://vm.ee/sites/default/files/Estonia_for_UN/ecuador_security_council_cyber_stability.pdf

53. See statements delivered by Ireland at Arria-formula Meeting on 'Cyber Stability, Conflict Prevention and Capacity-Building', hosted virtually on 22 May 2020, https://vm.ee/sites/default/files/Estonia_for_UN/200521_remarks_arria_meeting_on_cyber_final_written.pdf, and by Italy, https://vm.ee/sites/default/files/Estonia_for_UN/riunione_del_cds_in_formato_arria.pdf.

54. See Italy's statement, ibid., p. 2.

55. Statement by Canada at the Arria-formula meeting of the Security Council on cyber-attacks against critical infrastructure on 26 August 2020, https://www.youtube.com/watch?v=CbBchZEG5D8, at 2:05:20.

56. Statement by Izumi Nakamitsu, High Representative for Disarmament Affairs, Security Council open debate on the 'Maintenance of International Peace and Security in Cyberspace' on 29 June 2021, https://un.mfa.ee/wp-content/uploads/sites/57/2021/06/Nakamitsu-29-June.pdf.

57. Cyber Peace & Security Monitor, vol. 1, no. 7, 2020, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.7.pdf.

58. For an overview of the interviews conducted, see Annex.

59. Renata Hessmann Dalaqua, Kjølv Egeland, and Torbjørn Graff Hugo, "Still Behind the Curve: Gender Balance in Arms Control, Non-Proliferation and Disarmament Diplomacy", UNIDIR, p. 10, https://doi.org/10.37559/WMD/19/gen2.

60. Ibid.

61. UNIDIR, "Gender in Cyber Diplomacy", 2019, https://unidir.org/sites/default/files/2019-12/Gender%20in%20Cyber%20Diplomacy_Factsheet.pdf.

62. Ibid.

63. Australian Department of Foreign Affairs and Trade, "Women in International Security and Cyberspace Fellowship", press release, 2020, https://www.dfat.gov.au/sites/default/files/wic-fellowship-press-release.pdf.

64. Ibid.

65. Allison Pytlak, "A New 'Women in Cyber' Fellowship has a Big Impact on the OEWG", in Cyber Peace & Security Monitor, vol. 1, no. 7, 2020, p. 15, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.7.pdf.

66. General Assembly, UN document A/AC.290/2021/CRP.2, 10 March 2021, para. 12, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

67. UNIDIR, "Gender in Cyber Diplomacy", 2019, https://unidir.org/sites/default/files/2019-12/Gender%20in%20Cyber%20Diplomacy_Factsheet.pdf.

68. UN-Women, "Women, Peace & (Cyber) Security in Asia and the Pacific", 2020, p. 3, https://asiapacific.unwomen.org/en/digital-library/publications/2020/06/action-brief-women-peace-and-cyber-security-in-asia-and-the-pacific.

69. Security Council, UN document S/2020/946, 25 September 2020, p. 18, https://undocs.org/en/S/2020/946.

70. Alter, Charlotte. 2017. "U.N. Says Cyber Violence Is Equivalent to Physical Violence Against Women". *Time Magazine* https://time.com/4049106/un-cyber-violence-physical-violence/; Al-Alosi. 2017. "Technology-facilitated abuse: the new breed of domestic violence". *The Conversation*. https://theconversation.com/technology-facilitated-abuse-the-new-breed-of-domestic-violence-74683. "Gender Equality and Cybercrime/Cyber Violence", https://rm.coe.int/gender-mainstreaming-toolkit-15-gender-equality-and-cybercrime-cybervi/168092e9b4 ; Sharland, Lisa and Hannah Smith. 2019. "Cyber, Technology and Gender: What Are We Missing?". *The Strategist* https://www.aspistrategist.org.au/cyber-technology-and-gender-what-are-we-missing/; Sahana Dharmapuri and Jolynn Shoemaker, "Women, Peace and Security and the Digital Ecosystem", Our Secure Future, 2021, https://www.oursecurefuture.org/sites/default/files/WPS%20Digital%20Ecosystem.pdf.

71. These may be viewed as instances of 'semiotic violence'; see Alexis Henshaw, "Bringing Women, Peace and Security Online: Mainstreaming Gender in Responses to Online Extremism", Global Network on Extremism and Technology, 2021, https://gnet-research.org/wp-content/uploads/2021/03/GNET-Report-Women-Peace-And-Security.pdf.

72. Henri Myrttinen, "Connecting the Dots: Arms Control, Disarmament and the Women Peace and Security Agenda", UNIDIR, 2020, https://unidir.org/sites/default/files/2020-12/Connecting%20the%20Dots_0.pdf.

73. UN-Women, "Women, Peace & (Cyber) Security in Asia and the Pacific", 2020, https://

asiapacific.unwomen.org/en/digital-library/publications/2020/06/action-brief-women-peace-and-cyber-security-in-asia-and-the-pacific.

74. Ibid.

75. Table draws directly on the definitions provided in Linda Baker, Marcie Campbell and Elsa Barreto, "Understanding Technology-Related Violence Against Women: Types of Violence and Women's Experiences", Learning Network Brief 6, Centre for Research and Education on Violence Against Women and Children, Western University, 2013, http://www.vawlearningnetwork.ca/our-work/briefs/brief-06.html.

76. Those States which have not recently experienced conflict or are categorized as 'developed' often have had 'outward-looking' NAPS, rather than addressing issues of domestic concern (e.g. status of refugees, indigenous and displaced populations). However, this is starting to shift; see Security Council, UN document S/2020/946, 25 September 2020, p. 26, https://undocs.org/en/S/2020/946.

77. For 2020 indicators compiled by the International Telecommunication Union, see https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ITU_regional_global_Key_ICT_indicator_aggregates_Nov_2020.xlsx.

78. UN-Women, *Preventing Conflict, Transforming Justice, Securing the Peace: A Global Study on the Implementation of United Nations Security Council resolution 1325*, 2015, p. 202, https://reliefweb.int/sites/reliefweb.int/files/resources/UNW-GLOBAL-STUDY-1325-2015.pdf.

79. Security Council, UN document S/2020/946, 25 September 2020, p. 6, https://undocs.org/en/S/2020/946.

80. Security Council, UN document S/2019/800, 9 October 2019, https://undocs.org/en/S/2019/800; see also General Assembly, UN document A/74/821, 29 May 2020, p. 8, https://undocs.org/A/74/821.

81. Security Council, UN document S/2020/946, 25 September 2020, p. 20, https://undocs.org/en/S/2020/946.

82. Lucina Di Meco and Kristina Wilfore, "Gendered Disinformation is a National Security Problem", Tech Stream, 8 March 2021, https://www.brookings.edu/techstream/gendered-disinformation-is-a-national-security-problem/.

83. Hannah Smith and Katherine Mansted, "Weaponised Deep Fakes. National Security and Democracy", policy brief, Report No. 28, Australian Strategic Policy Institute, 2020, p. 5, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-04/Weaponised%20deep%20fakes.pdf.

84. Ian Sample, "What are Deepfakes—and How Can You Spot Them?", *The Guardian*, 13 January 2020, https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them.

85. Oliver Ward, "Sex and Deepfakes: Sexualised Misinformation will Hamper Future Female Democratic Participation", *ASEAN Today*, 21 November 2019, https://www.aseantoday.com/2019/11/sex-and-deepfakes-sexualised-misinformation-will-hamper-future-female-democratic-participation/; "Altered Image: Burma's Aung San Suu Kyi 'in Fake Headscarf'", *BBC News*, 9 June 2014, https://www.bbc.com/news/blogs-news-from-elsewhere-27740282; and Raphael Satter, "Deepfake Used to Attack Activist Couple Shows New Disinformation Frontier", *Reuters*, 15 July 2020, https://www.reuters.com/article/us-cyber-deepfake-activist/deepfake-used-to-attack-activist-couple-shows-new-disinformation-frontier-idUSKCN24G15E.

86. Naseem Tarawnah, "Sextortion, Harassment, and Deepfakes: How Digital Weapons are Being Used to Silence Women", IFEX, 5 March 2020, https://ifex.org/sextortion-harassment-and-deepfakes-how-digital-weapons-are-being-used-to-silence-women/; "Deepfake Poses a Threat to Human Rights Defenders in the Middle East", Gulf Centre for Human Rights, 14 October 2019, https://www.gc4hr.org/news/view/2227.

87. Agnes E. Venema, "Deepfakes as a Security Issue: Why Gender Matters", Women in International Security, 4 November 2020, https://www.wiisglobal.org/deepfakes-as-a-security-issue-why-gender-matters/.

88. Security Council, UN document S/2020/946, 25 September 2020, p. 24, https://undocs.org/en/S/2020/946.

89. Mehmet Ümit Necef, "'If Men Were Men, then Women Would be Women': ISIL's Construction of Masculinity and Femininity", Center for Modern Middle East and Muslim Studies, University of Southern Denmark, 2016, p. 4, https://www.sdu.dk/-/media/files/om_sdu/centre/c_mellemoest/videncenter/artikler/2016/necef+article+may+16.pdf.

90. Chantal de Jonge Oudraat and Michael E. Brown, "Women, Gender, and Terrorism: The Missing Links", policy brief, Women in International Security, 1 August 2016, pp. 3 and 6, https://wiisglobal.org/wp-content/uploads/2014/02/WIIS-Policy-Brief_Women-Gender-and-Terrorism-The-Missing-Links.pdf.

91. Elizabeth Pearson, "Online as the New Frontline: Affect, Gender, and ISIS-Take-Down on Social Media", *Studies in Conflict & Terrorism*, vol. 41, no. 11, 2018, https://doi.org/10.1080/1057610X.2017.1352280.

92. Ibid.

93. Sanchez, Sergio E., "The Internet and the Radicalization of Muslim Women", paper presented at the annual meeting of the Western Political Science Association, Seattle, 17 April 2014, p. 8, http://www.wpsanet.org/papers/docs/The%20Internet%20and%20the%20Radicalization%20of%20Muslim%20Women.pdf.

94. Maura Conway, Ryan Scrivens and Logan Macnair, "Right-Wing Extremists' Persistent

Online Presence: History and Contemporary Trends", policy brief, International Centre for Counter-Terrorism, October 2019, p. 2, https://icct.nl/wp-content/uploads/2019/11/Right-Wing-Extremists-Persistent-Online-Presence.pdf.

95. Counter-Terrorism Committee Executive Directorate, "Member States Concerned by the Growing and Increasingly Transnational Threat of Extreme Right-Wing Terrorism", CTED Trends Alert, April 2020, p. 5, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_trends_alert_extreme_right-wing_terrorism.pdf.

96. Manoel Horta Ribeiro et al. 2021. "The Evolution of the Manosphere Across the Web", *Proceedings of the Fifteenth International AAAI Conference on Web and Social Media*, 8¬–10 June 2021, p. 205, https://ojs.aaai.org/index.php/ICWSM/article/view/18053.

97. The Global Internet Forum to Counter Terrorism provides an example of a multi-stakeholder platform.

98. As an example, it could be noted that the Christchurch Call—for a commitment by governments and tech companies to eliminate terrorist and violent extremist content online—makes no reference to gender issues.

99. Deborah Brown and Allison Pytlak, "Why Gender Matters in International Cyber Security", Women's International League for Peace and Freedom and the Association for Progressive Communications, 2020, p. 6, https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf.

100. Ibid.

101. Ibid, p. 12.

102. Katharine Millar, James Shires, and Tatiana Tropina, "Gender Approaches to Cybersecurity: Design, Defence and Response", UNIDIR, 2021, https://doi.org/10.37559/GEN/21/01.

103. Susan Leavy, "Gender Bias in Artificial Intelligence: The Need for Diversity and Gender Theory in Machine Learning", *Proceedings of the First International Workshop on Gender Equality in Software Engineering*, Gothenburg, Sweden, 28 May 2018, https://doi.org/10.1145/3195570.3195580.

104. Katharine Millar, James Shires, and Tatiana Tropina, "Gender Approaches to Cybersecurity: Design, Defence and Response", UNIDIR, 2021, https://doi.org/10.37559/GEN/21/01.

105. Julia Slupska and Leonie M. Tanczer, "Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things", *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*, https://www.emerald.com/insight/

content/doi/10.1108/978-1-83982-848-520211049; See also Simon Parkin, et al. 2019, "Usability Analysis of Shared Device Ecosystem Security: Informing Support for Survivors of IoT-Facilitated Tech-Abuse", *Proceedings of the New Security Paradigms Workshop*, San Carlos, Costa Rica, 23–26 September 2019, https://doi.org/10.1145/3368860.3368861.

106. Gendered threat models may also be present at State level, such as in vulnerability equities processes. See Sven Herpig and Ari Schwartz, "The Future of Vulnerabilities Equities Processes Around the World", Lawfare, 4 January 2019, https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world.

107. World Economic Forum, "Assessing Gender Gaps in Artificial Intelligence", 2018, https://reports.weforum.org/global-gender-gap-report-2018/assessing-gender-gaps-in-artificial-intelligence/; UN-Women has noted that over 70 per cent of artificial intelligence professionals are men; see "Women, Peace & (Cyber) Security in Asia and the Pacific", 2020, p. 3, https://asiapacific.unwomen.org/en/digital-library/publications/2020/06/action-brief-women-peace-and-cyber-security-in-asia-and-the-pacific.

108. Surya Deva, "Addressing the Gender Bias in Artificial Intelligence and Automation", Open Global Rights, 10 April 2020, https://www.openglobalrights.org/addressing-gender-bias-in-artificial-intelligence-and-automation/.

109. Vyacheslav Polonski, "AI is Convicting Criminals and Determining Jail Time, but Is it Fair?", World Economic Forum, 19 November 2018, https://www.weforum.org/agenda/2018/11/algorithms-court-criminals-jail-time-fair/. Also see UN-Women, "Women, Peace & (Cyber) Security in Asia and the Pacific", 2020, p. 3, https://asiapacific.unwomen.org/en/digital-library/publications/2020/06/action-brief-women-peace-and-cyber-security-in-asia-and-the-pacific; World Bank, *World Development Report 2016*, 2016, p. 134, http://documents1.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf.

110. Sarah Shoker, "Making Gender Visible in Digital ICTs and International Security", report commissioned by Global Affairs Canada, 2020, p. 6, https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf.

System Update: Towards a Women, Peace and Cybersecurity Agenda

Designed by Jan Ondrasek

System Update explores the relationship between the Women, Peace and Security (WPS) agenda on the one hand and cyber-enabled threats and cybersecurity on the other. The paper analyses the linkages between WPS priority themes—gender equality, women's participation in international security, prevention and protection of violence against women, gender-differentiated needs—and international cybersecurity. It identifies priority areas that should be addressed to ensure a gender-inclusive cyberspace that protects the rights of women and girls.