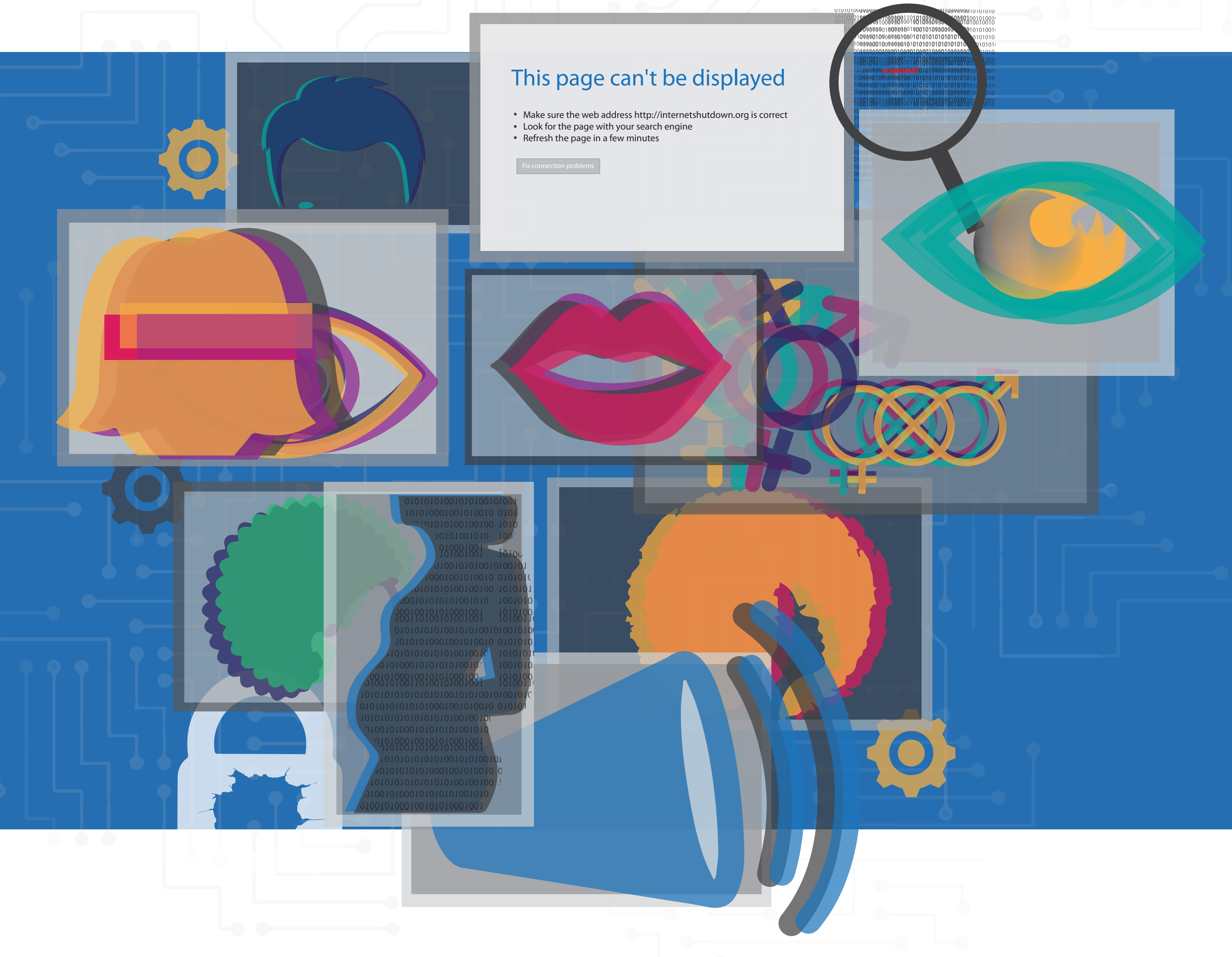
APC
ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS

WOMEN'S INTERNATIONAL LEAGUE FOR PEACE & FREEDOM


This page can't be displayed
• Make sure the web address http://internetshutdown.org is correct
• Look for the page with your search engine
• Refresh the page in a few minutes
Fix connection problems

Why Gender Matters in International Cyber Security

April 2020

Why Gender Matters in International Cyber Security

First edition
28 pp.

Authors: Deborah Brown and Allison Pytlak
Cover illustration: Cathy Chen
Design: Nadia Joubert

www.wilpf.org
www.reachingcriticalwill.org
www.apc.org

This research was made possible in part by a financial contribution by Global Affairs Canada.

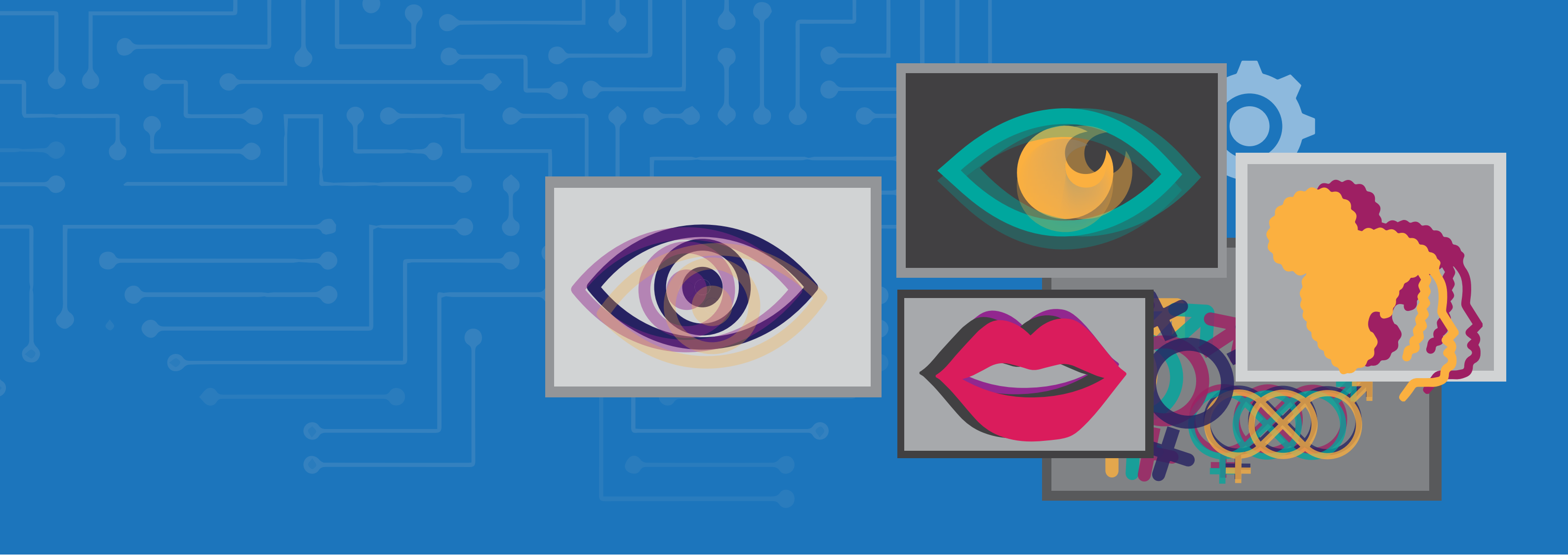


Table of Contents

Section I: Introduction

Gender matters in international cyber security. It shapes and influences our online behaviour; determines access and power; and is a factor in vulnerability, whether real or perceived. As a result, malicious cyber operations can differently impact people based on their gender identity or expression. Online gender dynamics have been shown to reinforce or even amplify the social, economic, cultural and political structures of the offline world. As gender affects the way people and societies view weapons, war, and militarism, a gender analysis of international cyber security can generate more nuanced understandings of the dynamics which shape policy and practice in this area.

Yet, much of what is known about gender and cyber security comes from studies of online gender-based violence (GBV) and gender inequality within the information and communications technology (ICT) sector. There is growing recognition that online GBV is rooted in historical and structural inequalities in power relations between genders, which needs to be addressed as part of broader efforts to realize women's human rights. At the international level, human rights and 'international security' are sometimes kept separate, meaning that while human rights should be a consideration when discussing international cyber security[1], the reality is that this has rarely been the case. As a result, less is known about how malicious international cyber operations between states affect people differently on the basis of gender or other characteristics that may put them in positions of vulnerability. While great strides have been made in recognizing the applicability of the human rights framework to threats and abuses against women's digital contexts, including though resolutions and recommendations from authoritative human rights bodies, the gender dimensions of international cyber security remain nearly unexplored.

This report aims to fill that gap. It will have relevance for those working in or studying international cyber security policy, diplomacy, or research as well those interested in the nexus of gender and security. This report, commissioned by Global Affairs Canada, should help to inform recommendations for how multilateral cyber security processes, in particular the United Nations' (UN) Open-ended working group (OEWG) on 'Developments in the field of information and telecommunications in the context of international cyber security' and participating member states can incorporate a gender perspective into future work. It opens by presenting key gender-relevant terms and concepts, alongside relevant frameworks in order to establish a common baseline of knowledge among readers. The subsequent sections use both desk and original research in the form of interviews to consider what are the potential impact of international cyber operations, in particular internet shutdowns, data breaches, and disinformation campaigns. The third section explores gender diversity and women's participation within cyber policy and diplomacy.

There are some limitations to highlight for readers at the outset. While the subsequent section will unpack terms and concepts that relate to gender, the original research found in later sections of the report focus exclusively on the experiences of women (except where otherwise noted). The researchers fully acknowledge and support the importance of approaching this topic with the wider lens, but because of time and other constraints were unable to examine the broader spectrum of people who may be impacted in relation to their gender identities and expressions. More research in this area should be encouraged. For similar reasons, the research does not include girls in its consideration of gender. The section on participation focuses mainly on the policy and diplomatic sectors within cyber security, and less on technical roles. Finally, the report assumes that readers have more familiarity with cyber security than gender. The researchers relied on desk research and interviews, conducted over a two-month period. Our methodology is detailed at the start of sections III and IV.

[1] Deborah Brown and Anriette Esterhuysen, "Why cybersecurity is a human rights issue, and it is time to start treating it like one", Association for Progressive Communications, 28 November 2019, https://www.apc.org/en/news/why-cybersecurity-human-rights-issue-and-it-time-start-treating-it-one

Section II: Framing

Gender perspectives are being more readily accounted for and discussed in multilateral peace and security forums that have traditionally addressed security from a state-centric and militaristic lens. This is a positive step forward but in order to be impactful, it's important to have clarity and common understanding of key terminology and concepts, in order to avoid their conflation or misuse.

To begin, gender is not interchangeable with biological sex (i.e. male, female, intersex). Gender refers to the roles, behaviours, activities, attributes and opportunities that any society considers appropriate for girls and boys, and women and men. Gender interacts with, but is different from, the binary categories of biological sex.[2] Significantly, gender constructs determine who holds power, whether in families, societies, and even in global affairs.[3]

As such, a gender analysis, sometimes described as applying a gender perspective, can illuminate important patterns within armed violence and conflict, and how it is differently experienced as based on gender. This in turn can help inform policies and programs that specifically address these challenges. A gender analysis asks questions about how an experience is different for someone on the basis of their gender identity, and also examines relationships between genders, including what that means for power, access, and limitations.

To use an offline example: it is well-established that there is a strong correlation between gun cultures and perceptions of manliness. In fact in the United States (US) a statistical correlation between domestic violence and mass shootings has also been documented.[4] Cultural norms of masculinity have long denoted men as protectors and as warriors in ways that encourage violence and often, the use of guns, whether as soldiers or in the context of urban gang violence.[5] Acknowledging this enables policy and programmatic responses that focus on addressing violent masculinity as a root cause of violence and gun cultures, in addition to reducing access to and availability of weapons.

In the digital space, gender analysis can reveal the power dynamics which influence, for example, why there is a preponderance of men working in cyber security fields, and how offline inequalities are exacerbated through growing gender digital divides.[6] There is also a gender dimension present in data collection and surveillance[7], as activities that are inherently about labeling and categorising individuals through methods are often predicated on existing binary gender norms. Systems developed by such data can be exploited in ways that either perpetuate such norms—for example, by contributing to unrealistic expectations of female beauty or binary definitions of gender—or to limit access and discriminate against those who do not conform.

Violence that is perpetrated against a person on the basis of gender is known as gender-based violence (GBV). Acts of GBV violate a number of human rights principles enshrined in international instruments and can constitute violations of international humanitarian law (IHL) if perpetrated during armed conflict.[8] There are four generally recognized forms of GBV: physical, sexual, psychological/emotional, and economic, although others are increasingly being recognized as well.

[2] World Health Organization, https://www.who.int/health-topics/gender

[3] UN Women, https://www.un.org/womenwatch/osagi/conceptsandefinitions.htm

[4] Jane Mayer, "The Link Between Domestic Violence and Mass Shootings", *The New Yorker,* https://www.newyorker.com/news/news-desk/the-link-between-domestic-violence-and-mass-shootings-james-hodgkinson-steve-scalise

[5] Henri Myrttinen, "Disarming Masculinities", *Disarmament Forum: Women, Men, Peace and Security,* UN Institute for Disarmament Research, Vol. 4, pp. 37–46.

[6] International Telecommunication Union, "Bridging the gender divide", https://www.iatu.int/en/mediacentre/backgrounders/Pages/bridging-the-gender-divide.aspx

[7] Privacy International, *From Oppression to Liberation: Reclaiming the Right to Privacy,* November 2018, https://www.privacyinternational.org/report/2457/report-oppression-liberation-reclaiming-right-privacy. https://www.apc.org/sites/default/files/APC_submission_Gender_Perspectives_on_Privacy_Oct_2018.pdf

[8] Ray Acheson, *Gender-Based Violence and the Arms Trade Treaty,* 2015, p.6, http://www.reachingcriticalwill.org/resources/publications-and-research/publications/10112-gender-based-violence-and-the-arms-trade-treaty

GBV tends to have a disproportionate impact on women and girls, due to their subordinate status in society and vulnerability to violence, but this does not mean that all victims of gender-based violence are women. Men and boys, trans or intersex people, may also be victims of GBV, and it can also be conducted against individuals on the basis of sexual orientation and gender identity; in fact, men and boys tend to be targeted for GBV when their sexual orientation or gender identity diverges from gender norms Therefore, violence against women (VAW) fits within and constitutes GBV but is a narrower and more limited term.

Online GBV is an act of GBV that is committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as mobile phones, the internet, social media platforms, and email. Online GBV tends to mirror and exacerbate gender norms and inequalities of the offline world.[9] It is often directed at those who break from—or are perceived as breaking from—traditional gender norms in any range of ways, whether it be sexual orientation or gender identity, choice of profession, physical appearance, lifestyle, athletic or intellectual ability, or political views, as just some examples. Non-conforming behaviour frequently becomes the focus of abuse; a lot of trolling, for example, uses language and insults that are highly gendered—misogynist or anti-gay rhetoric, threats of rape, etc. With the emergence of social media in particular, sexual and intimate partner violence have taken on new dimensions that include bullying, defamation, impersonation, surveillance, tracking, and harassment as well as non-consensual sharing of photos or messages.

Finally, there are also important distinctions to be made between gender diversity, equality, equity, parity, and women's participation. Sometimes these terms are used interchangeably within UN settings or are selected for use deliberately because of their respective and perceived political viability, in that some may be considered as more 'ambitious' than others, or touch on cultural sensitivities. Diversity would encourage just that—space for the views and inputs of individuals on the basis of diverse identifying features or attributes; in this case gender but which could include other intersecting characteristics. Parity has often been used to advocate for a 50/50 participation ratio between two sexes in a given setting. Somewhat similarly, equality emphasizes that all genders receive the same resources or rights; whereas equity means fairness of treatment for all genders according to their respective needs. Women's participation lifts up the involvement of women alone and is necessary for women's equity, in that participation means that women themselves can identify their unique needs, but also contribute experiences and perspectives so that any policy (or other) output works for the women it impacts. Participation is one of four 'pillars' of the Women, Peace and Security (WPS) Agenda established by UN Security Council Resolution 1325, outlined in Annex I, yet is sometimes overshadowed by other of the pillars, notably the 'protection pillar'.

Understanding the Normative Landscape

There are relevant instruments, agendas, and frameworks that policymakers in global cyber security can draw from when seeking to advance a gender perspective within multilateral cyber security, either as a source of information or to establish policy coherence with states' existing commitments to gender equality.

This includes the WPS Agenda, as established by UN Security Council resolution 1325 and WPS National Action Plans; the Beijing Declaration and Platform for Action; the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW Convention); the 2030 Agenda; UN Human Rights Council (HRC) Resolution 38/5; outcome documents of the World Summit on the Information Society; International Telecommunication Union (ITU) Resolution 70; and the Feminist Principles of the Internet, developed by the Association for Progressive Communications (APC). These are all outlined in Annex I.

[9] *Online gender-based violence: A submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences,* November 2017, https://www.apc.org/sites/default/files/APCSubmission_UNSR_VAW_GBV_0_0.pdf

In Focus: A gender analysis of the 2015 UN cyber norms

The 2015 UN Group of Governmental Experts (GGE) on advancing responsible state behaviour in cyberspace in the context of international security issued a consensus report, which[10] *outlines eleven recommendations for voluntary, non-binding norms and principles for responsible state behavior in cyberspace. These were endorsed by the UNGA and now form a baseline for discussion in the UN OEWG.*

As already explained, a gender analysis asks questions to reveal underlying gender and power dynamics and differentials in any given situation. Common questions would include: Where are the women, girls, men, boys in this context? What are they doing? Which women, girls, men, boys? What are their respective needs, interests, and vulnerabilities? What are structural power relations between and among them?

A gender analysis of the eleven norms and principles reveals the following guidance for a more gender-sensitive approach to their implementation:

- *Define "critical infrastructure" in ways that are human-centric and holistic. Recognize that a breakdown or loss of different critical infrastructures would be experienced differently on the basis of gender. (Norms f, g, and h)*
- *Build understanding of the gender components of the Human Rights Council and General Assembly resolutions referenced in norm e, as well as of newer iterations of those resolutions*[11] *and who they link to the mandates of the OEWG and GGE. These resolutions, as well as the 2018 HRC resolution, "Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts" (38/5) outline existing state commtments to promoting and protecting women's human rights, which have linkages to the differential harms women face in the context of international cyber incidents (as explored in this report).*
- *In applying measures to increase security and stability of ICT practices (norm a), states should acknowledge that threat models and what is deemed harmful is informed by gender.*
- *When considering all relevant information in the case of an ICT attack (norm b), states include research into possible gendered impacts, and work inclusively with all stakeholders to understand the larger context of an ICT incident, including its impact on the enjoyment of women's rights.*
- *Capacity-building or other measures to build a global culture of cyber security to protect critical infrastructure (norm g) should be developed inclusively with full participation by a diverse set of women and LGBTIQ individuals and seek to illuminate the gender dimensions of cyber security operations.*

[10] UN General Assembly, *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,* Resolution A/70/174, 22 July 2015, https://undocs.org/A/70/174

[11] The 2016 and 2018 versions of the HRC resolution on the *Promotion, protection and enjoyment of human rights on the internet* (32/13 and 38/7) condemn online gender-based attacks and include calls to bridge the gender digital divide. The 2018 UNGA resolution on *Privacy in the digital age* (73/179) included calls on states to consider developing, reviewing, implementing, and strengthening gender-responsive policies that promote and protect the right of all individuals to privacy in the digital age.

Section III: Differentiated Impact of Cyber Incidents on the Basis of Gender

It is well established that women are uniquely and disproportionately affected by conflict and other threats to international peace and security. While men are often the main combatants, women are impacted in less visible ways or are targeted for being women.[12] There is, however, little data on how this differentiated impact can be better understood and addressed within the field of ICTs in the context of international security. This section aims to address this question. Before addressing the specific needs and threats faced by women in potential conflicts in cyberspace, it is necessary to contextualize women's differential experiences in their use of ICTs.

First, women do not enjoy equal access to ICTs. According to the ITU, in 2019, the proportion of women using the internet globally was 48 percent, compared to 58 percent of men.[13] While in some regions, such as the Americas, the gender gap is nearly zero, and in others, such as the former Soviet countries and Europe, it is shrinking, in many parts of the world—in particular the Arab States, Asia, the Pacific, and Africa—the gender gap has actually grown between 2013 and 2019. Women's ability to gain meaningful internet access[14] is influenced by factors including location, economic power, age, gender, racial or ethnic origin, social and cultural norms, and education, amongst other things.[15] Disparity and discrimination in these areas translate into specific gender-based challenges and barriers to meaningful access.

For example, in India it is critical to look at the context and how access to the internet is gendered. Ninety percent of people access the internet through a mobile device, with families typically having one device, access to which is controlled by a man. There are time limitations on when women can use the device and content limitations on what women can access. Some uses of mobile connectivity that are gendered include relying on devices to reach out to family, ordering a ride sharing service when feeling unsafe, and for educational purposes.[16] Multiple interviews conducted for this section of the research stressed the importance of situating the differential way women experience threats in cyberspace in the underlying and more fundamental gender divides that are located within economic, social, political, and cultural contexts that recognize existing inequalities, which among other things, includes unequal access to the internet. Taking an intersectional approach was also emphasized, given that gender is one of many critical factors that impacts how people experience threats in cyberspace. Location (urban vs. rural) socioeconomic levels, and political stability/instability are also key.

Second, threats women face in cyberspace cannot easily or neatly be separated from their offline lived realities. Online GBV is experienced on a continuum, as is demonstrated by the fact that the online doxxing of women can result in-person rape and death threats and even bomb scares.[17] Even when there is a data breach or intentional disclosure of personally identifiable information that is not targeted at women, women can experience differential impacts because of underlying inequality and discrimination.

[12] See, for example, *Women, Peace and Security: Study of the UN Secretary-General pursuant to UN Security Council Resolution 1325*, 2002 and UN Office for the Coordination of Humanitarian Affairs, *Global Humanitarian Overview* 2019, p. 17.

[13] ITU Backgrounder, "Bridging the gender divide", https://www.itu.int/en/mediacentre/backgrounders/Pages/bridging-the-gender-divide.aspx

[14] "Meaningful internet access" should be construed as pervasive, affordable connectivity (of sufficient quality and speed) to the internet in a manner that enables the user to benefit from internet use, including to participate in the public sphere, exercise human rights, access and create relevant content, engage with people and information for development and well-being, etc.; irrespective of the means of such access (i.e. whether via a mobile or other device; whether through private ownership of a device or using a public access facility like a library). See https://www.intgovforum.org/multilingual/index.php?q=filedepot_download/3406/437

[15] A. Milek, C. Stork and A. Gillwald, "Engendering communication: A perspective on ICT access and usage in Africa", *Info: The Journal of Policy, Regulation and Strategy for Telecommunications, Information and Media,* 13(3), 2011, pp. 125-141.

[16] Interview with Mishi Choudhary, Legal Director, Software Freedom Law Center, February 6, 2020.

[17] N. Wingfield, "Feminist Critics of Video Games Facing Threats in 'GamerGate' Campaign", 15 October 2014, https://www.nytimes.com/2014/10/16/technology/gamergate-women-video-game-threats-anita-sarkeesian.html?_r=

Take, for example, the 2017 publishing by WikiLeaks of massive databases containing sensitive and private information of millions of ordinary Turkish citizens, which included a special database of almost all adult women in Turkey.[18] WikiLeaks did not appear to have an agenda to put women at risk in publishing this information. But as Turkish sociologist Zeynep Tufekci put it, "We are talking about millions of women whose private, personal information has been dumped into the world, with nary an outcry. Their addresses are out there for every stalker, ex-partner, disapproving relative or random crazy to peruse as they wish. And let's remember that, every year in Turkey, hundreds of women are murdered, most often by current or ex-husbands or boyfriends, and thousands of women leave their homes or go into hiding, seeking safety." In considering the specific needs of women related to cyber security threats and potential conflicts in cyberspace, it is critical to understand that while the threats may be perpetrated or exacerbated through technology, they must be situated in underlying power dynamics and inequalities.

Finally, it is important to note that in many contexts, use of the internet is gendered, and in some cases when they have access, women may be more reliant on the internet. For example, women may be particularly reliant on the internet for earning income or pursuing an education (if for example their responsibilities in the home prevent them from doing so offline), for expressing themselves (especially when it comes to expression or content that is taboo, such as sexual expression or defying gender stereotypes), for accessing information relating to their sexual and reproductive health and rights (which may not be accessible offline),19 for seeking out services that enhance their physical safety (for example ride hailing and domestic violence services), and for exploring their sexual orientation of gender identity (which may be criminalized or stigmatized if done openly offline). Therefore, threats in cyberspace can have a compounding effect on women because of the empowering effect the internet can have for them.

> ***In Focus – LGBT people's use of the internet***
>
> *The internet, in part because of the degree of anonymity it can provide, enables individuals and minority groups to associate on sensitive matters, including sexual orientation.*[20] *It creates enabling environments for people to share and seek sensitive information and engage in online associations based on identities which can be illegal in some countries, such as sexual orientations or gender identities. Marginalised or persecuted sexual minorities find spaces for exercising their freedom of expression and association more privately in online spaces as compared to offline spaces. For example, dating apps tailored to LGBT people can provide a unique space to communicate within a safe community without the persecution or stigma that may be experienced in other dating methods. It is therefore crucial that LGBT people have access to tools that enable them to protect the confidentiality of digital communications to ensure their enjoyment of human rights. A global survey conducted by APC as part of the EROTICS (Exploratory Research on Sexuality and the Internet) project*[21] *revealed that "the internet is considered an 'important' or 'very important' medium of sexual expression by 66 percent of the sample (among them, 39% consider it 'very important')."*[22] *However, while the internet*

[18] Z. Tufekci, "WikiLeaks Put Women in Turkey in Danger, for No Reason (UPDATE)" 25 July 2016 (Updated 6 December 2017) https://www.huffpost.com/entry/wikileaks-erdogan-emails_b_11158792

[19] Example from Bachchao project research: The reference material a researcher needed for her dissertation on women's studies was not available at the local public library, university or other avenues, which prompted her to search for it on Archive.org. The researcher also gave the example of using YouTube to get videos, which are helpful for adolescent girls, on topics like menstrual hygiene. One respondent in her early twenties said that she watches videos on YouTube to expand her knowledge of handmade embroidery and to learn to use new machines. Both examples illustrate that young women actively use the Internet for gaining knowledge, nurturing their ambitions and learning the skills that contribute to their livelihood. See: Chinmayi S K and Rohini Lakshané, *Of Sieges and Shutdowns: How unreliable mobile networks and intentional Internet shutdowns affect the lives of women in Manipur,* The Bachchao Project, 2018 http://thebachchaoproject.org/wp-content/uploads/Of_Sieges_and_Shutdowns_The_Bachchao_Project_2018_12_22.pdf

[20] APC, *The right to freedom of expression and the use of encryption and anonymity in digital communications: Submission to the United Nations Special Rapporteur on the right to freedom of opinion and expression,* 2015, https://www.apc.org/sites/default/files/APC%20submission%20to%20SR%20FOEX_20150211_0.pdf

[21] EROTICS is a network of activists and researchers working at the intersections of sexuality and the internet. More information at: https://erotics.apc.org/about-erotics

[22] H. Vale, "Body as data: EROTICS exploratory research on sexuality, rights and the internet", https://slides.com/hvale/body-as-data-dataveillance-the-informatisation-of-the-body-and-citizenship#/1

> *is an essential tool to communicate and spread critical information regarding LGBTIQ activism, these activists also face significant threats online: "the most frequent is harassment (75%), followed by intimidating online comments (63%) and blocked websites or filtering software that prevented the user from accessing information (54%)."* [23]
>
> *An interview conducted for this research with a person from Iran, who wishes to remain anonymous, demonstrates just how critical the internet can be for LGBTQ people in an environment in which their very identity is criminalized. In this person's words, "After coming to terms with my identity and orientation I did what I knew best: I established a network through which we tried to provide support to LGBTQ people. Our work included translation and online distribution of pamphlets, along with offering some support to those who were facing problems at home. You certainly know how things are in Iran. Parents usually get oppressive and violent when their kids come out. Even if they don't, the coming out process is complicated. Both parents and their kids need guidance which was (and is) nonexistent in Iran. Most people do not have access to queer-friendly sources of information. This gets worse especially when people come from less well-off backgrounds. They haven't got proper English training and Persian sources were, and I think still are, scarce. We also used to provide some help to transgender people. At the time we used Yahoo Messenger for communicating. Using the service we were able to prevent a few self-harm incidents by simply listening to the people."* [24]

Internet Shutdowns

While internet shutdowns are primarily used as a tool by governments against people under their jurisdiction, they have also been used as a tactic during conflict against other populations, such as Russia's 2016 shutdown of the internet in Crimea[25] and by cybercriminals, who have launched cyberattacks across borders, such as the attack that took Liberia offline in 2016.[26] Because internet shutdowns conducted by a government domestically are much more common and better documented, the researchers were able to study the gender dimensions of this phenomenon, from which it is possible to extrapolate the gendered impact of internet shutdowns when carried out in the context of international cyber conflict.

The methodology for this section relied on a combination of desk research and interviews, with a heavy reliance on the latter given there is very little published on the gender dimensions of internet shutdowns, despite the practice being widespread. The researchers compiled a list of all the internet shutdowns documented in 2018 and endeavored to interview people who either experienced those shutdowns or conduct research or advocacy around those shutdowns. Time constraints meant that it was not possible to interview people from each country that experienced shutdowns, so the researchers aimed to reach countries from different regions and political contexts. Interviewees were a mix of people who experienced shutdowns firsthand, and those who work on the issue (as journalists, researchers or advocates) in or from the countries in question. All interviewees were women, with the exception of a queer person from Iran, who spoke on the condition of anonymity. Countries covered by the interviews were: Cameroon, Democratic Republic of Congo (DRC), Ethiopia,[27] India (2), Iran (2), Pakistan, and Venezuela. One interviewee covered the issue globally, as she led a global campaign to counter internet shutdowns. The shutdowns covered in this research are not representative or in any way comprehensive but shed light into the different ways that internet shutdowns can affect women.

[23] APC, *EROTICS Global Survey 2017: Sexuality, rights and internet regulations,* https://www.apc.org/sites/default/files/Erotics_2_FIND-2.pdf.

[24] Anonymous interview, February 20, 2020.

[25] Hayes Brown, "Russia Cuts Off the Internet in Crimea," 11 August 2016, https://www.buzzfeednews.com/article/hayesbrown/russia-cut-off-the-internet-in-crimea

[26] Dominic Casciani, "Briton who knocked Liberia offline with cyber attack jailed", 11 January 2019, https://www.bbc.com/news/uk-46840461

[27] The interviewee from Ethiopia has expertise on internet shutdowns globally as the lead of the KeepItOn campaign, so her contribution to this research extended beyond Ethiopia.

Internet shutdowns can be defined as "an intentional disruption of internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information."[28] The UN Human Rights Council (HRC) has unequivocally condemned "measures to intentionally prevent or disrupt access to or dissemination of information online in violation of international human rights law" and called on all States to "refrain from and cease such measures."[29] The shutdowns covered in this research include years-long shutdowns as well as shorter ones, bans on popular social media and communications platforms and total communication blackouts, and shutdowns occurring in times of conflict and other forms of political turmoil.

For the most part, internet shutdowns are blunt tools that hit entire communities. However, because of power differentials in society and the specific ways that women use the internet, research conducted found that there were gendered impacts of internet shutdowns studied. A comment from an interviewee from Venezuela captured this well:

> *"I feel that due to certain gender roles, women are affected differently, particularly in Venezuela. We are left with a lot of the caregiving responsibilities – take care of the food, paying the bills – and in these situations [shutdowns] our ability to solve certain problems is restricted. Having access to certain information is key – during a blackout, my sister won't know if she should take her daughter to school or not, and my friend won't have a way of checking in with her boss since she telecommutes, thus facing the possibility of being fired and not being able to provide for her children since she's a single mom."* [30]

A few themes emerged concerning the ways in which gender impacted women's experiences of internet shutdowns: personal safety, professional/economic impact, emotional wellbeing, education, and connectivity.

Personal safety

A common theme from interviewees and existing literature is that mobile phones increase the perceived levels of security among women outside their homes and in public places. The study "Of Sieges and Shutdowns: How unreliable mobile networks and intentional Internet shutdowns affect the lives of women in Manipur'' interviewed women in northeast India and found "[h]aving a phone is a way of feeling secure. When in 2006, there were not many mobile phones in Manipur, we were doing focus group discussions with women on the status of security of women. One of the outcomes was [that] women would feel safe if they had a mobile phone. But we did not think that it would turn [into] a reality in 2016 where every woman has a phone. Today it's a better situation because women can inform their family members if they are going to be late or if they go out." [31]

Physical violence against women in publicis a common phenomenon in many parts of the world. An interviewee gave the example of a contact in Tehran who is a single woman in her 30s, who lives near an area that was quite violent during the protests in late 2019, where women were getting arrested and assaulted. When the government shut down the internet during the protests, it left the woman without the ability to be in contact if anything happened to her.The respondent was worried about her contact's safety. The woman in Tehran reported feeling isolated and afraid to go out.[32] In Pakistan's Federally Administered Tribal Area, or FATA, which has experienced an internet shutdown since 2016, people could go to internet cafes before fixed broadband was cut, but men make it difficult for women to go to internet cafes by creating a very hostile environment.[33]

[28] Berhan Taye, *Targeted, Cut-Off and Left in the Dark: Report of Global Shutdowns,* Access Now, 2019. https://www.accessnow.org/keepiton/#problem

[29] Human Rights Council, *The promotion, protection and enjoyment of human rights on the Internet,* Resolution A/HRC/RES/32/13, 18 July 2016, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/32/13

[30] Interview with Marianne Diaz, Analista de Políticas Públicas Derechos Digitales, 17 February 2020.

[31] S K Chinmayi and Rohini Lakshané, *Of Sieges and Shutdowns: How unreliable mobile networks and intentional Internet shutdowns affect the lives of women in Manipur,* The Bachchao Project, 2018 http://thebachchaoproject.org/wp-content/uploads/Of_Sieges_and_Shutdowns_The_Bachchao_Project_2018_12_22.pdf

[32] Interview with Mahsa Alimardani, Internet researcher that specialises in Iran and the Middle East, 29 January, 2020.

[33] Interview with Hija Kamran and Amel Ghani, Program Managers at Media Matters for Democracy, Pakistan, 3 February 2020.

An interviewee from India noted:

> *"The intersectional impact of a shutdown impacts women differently, especially in Delhi which continuously reports high number of cases of violence against women and sexual harassment. Most of the time, as a woman I share my live location during late night travel or when visiting an area less traveled. Further, since I personally visit social protests to report on them, keeping in contact with my colleagues and family becomes important. With the internet being suspended, reaching out for help becomes difficult. Further, during protests, minorities depend hugely upon community support, which is usually achieved through online messaging platforms. Not being able to use that is hugely restraining."* [34]

During partial internet shutdowns, people may be able to find ways to access the internet, but may not have access to the full range of communication channels that they rely on. For people who rely on secure communications channels because of their sexual orientation or gender identity, for example, being cut off from encrypted communications can be a threat to their safety. "When you are doing what I am doing, you need to constantly be cautious about your communications. Every personal contact can be used against you. In a country where gay relationships are criminalized, not having access to encrypted communication services is scary and life-threatening." [35]

Professional/economic impact

There are a number of efforts to measure the economic costs of shutdowns, much of which is guesswork in part because so much of the informal sector is typically not included in such measurements. A number of interviews identified women's use of e-commerce as having a negative impact on their financial well-being when the internet is shut down. For example, in Iran women sell and distribute handcrafts and homemade food through online platforms for industry/e-commerce (Facebook and Telegram)[36]. Internet shutdowns disrupted this. In Cameroon and Ethiopia, women specifically use Whatsapp/Telegram groups to sell household items (such as hair products and spices), outside of the mainstream/formal sector. During shutdowns, they are unable to sell their products.[37] A respondent from DRC similarly noted that women in the informal economy rely heavily on mobile communications to send and receive money.[38]

For women working in the formal economy, especially in sectors dominated by men, they expressed feeling their work and professional achievement was compromised because of internet shutdowns. In fact, both women who expressed this in interviews ultimately decided to leave where they were living, in part because of the impact of the disruptions on their professional life.

An independent woman journalist in Manipur, India who relies heavily on the internet for her work lamented that internet shutdowns affect her work. She explained that as a woman one is already at a disadvantage, and that in a competitive environment where opportunities for women are scarce, internet shutdowns additionally hamper one's work which has long term effects. In her words, "You miss opportunities… when your connectivity is hampered, your sense of independence is also affected. One may say it affects all… but as [a] woman you feel additionally frustrated, as your sense of empowerment or freedom is being affected…[the] internet gives me a sense of empowerment or say, opportunity to access information, opportunity to network, [I] send my stories across many places and get information from many places. Now, when you don't have access, when the net shuts down you feel disconnected, feel helpless, disempowered. [The] Internet give[s me an] advantage, the edge, and when that is curtailed one feels frustrated and disempowered, all the more as a woman." [39]

[34] See: Software Freedom Law Centre's Internet Shutdown Tracker: https://internetshutdowns.in.

[35] Anonymous interview, 20 February 20 2020.

[36] Interview with Mahsa Alimardani, Internet researcher that specializes in Iran and the Middle East, 29 January 2020.

[37] Interview with Berhan Taye, Senior Policy Analyst, Access Now, 10 February 2020.

[38] Interview with Annie Matundu-Mbambi, Chairwoman, WILPF DRC, 24 January 2020.

[39] Interview with Ninglun Hanghal, independent journalist, 18 February 2020.

A civil society activist from Venezuela shared similar frustrations and concerns:

> *"[T]hese constant issues with accessing the internet freely were the main reason why I had to leave Venezuela. I was already working as a researcher for Derechos Digitales and it had become impossible to hold a conference call, to research a paper or to stay on top of emails with less than four hours of reliable internet access a day. I had to face the choice of leaving my work or leaving the country, which was possibly the hardest choice I've had to make in my life."* [40]

Emotional well-being

Harm to emotional well-being is a commonly expressed response to internet shutdowns, both by people experiencing the shutdown and by people in the diaspora.

A woman who experienced an internet shutdown in 2016 in Manpur, India said, "For 15-20 days we could not communicate [with anyone]. No emergency cases happened. But it was scary because we could not communicate with people even when they go to [the] bazaar or if they were late from a travel. There was insecurity and fear."[41]

As an article on the prolonged shutdown in FATA in Pakistan put it, "Women, already deeply vulnerable in Pakistani society at large, are even more oppressed in the tribal areas. Their mobility is very restricted—and now the roads to information have been shut to them. Moreover, many men from FATA move to Gulf states to work as manual laborers on construction sites. Before the shutdown, local entrepreneurs started internet cafes that people could use to talk to their family members abroad. Now that those cafes don't exist anymore, people are forced to go months without talking to family members."[42]

Interview respondents who live outside their country (Iran and Venezuela) reported emotional distress at not being able to be in touch with their relatives, especially their female relatives during times of social/political unrest. "I am the provider/caregiver for my family back in Venezuela, so this means that when they are incommunicado this affects me severely, not only in a logistical manner, but also affects my mental health in a severe way."[43]

A queer person in Iran echoed this sentiment: "If I were to describe the experience in one word I would say, suffocating…young queer Iranians have been able to establish a support network using social media platforms. There are several Iranian news outlets and activists that are publishing LGBT-friendly information as well. The internet shutdown cut off the minority from a source of information and moral support. Everyone was affected by the blackout but queer people were more panicked. They were feeling a sense of isolation. Even amid natural disasters, people find time for love. Without the internet, the chances of meeting another queer person and hitting it off with them is close to zero in oppressive countries like Iran. Furthermore, online services like Telegram and WhatsApp provide people with a secure line of communication. During the shutdown, we were back to old-school telephony services and text messages which are monitored by state authorities. The encrypted messaging apps provide people with a sense of privacy the blackout put an end to that as well."[44]

Impact on education

Beyond impacts on safety, work, and emotional well-being, the research found that there was a gendered dimension to education during shutdowns. For example an interviewee in FATA noted that the shutdown affected people similarly, but because of patriarchy and cultural issues, there are/were differential effects. For example, women don't have much access to education throughout Pakistan, and in the tribal regions in particular. The internet helped women access education, and now that it's off, men still have access to schools, but women do not. Women had to drop out of schools/colleges.[45]

[40] Interview with Marianne Diaz, Analista de Políticas Públicas Derechos Digitales, 17 February, 2020.

[41] Bachchao Project.

[42] Hija Kamran, "A Year Without the Internet", 21 August 2017, ahttps://slate.com/technology/2017/08/the-internet-has-been-shut-down-in-pakistans-fata-for-more-than-a-year.html

[43] Interview with Marianne Diaz, Analista de Políticas Públicas Derechos Digitales, 17 February, 2020.

[44] Anonymous interview, February 20, 2020.

[45] Interview with Hija Kamran and Amel Ghani, Program Managers at Media Matters for Democracy, Pakistan, 3 February 2020.

Finding connectivity during a shutdown

Finally, in cases where the shutdown is partial, for example only covering mobile data, people go to public spaces, universities, and hotels and pay in order to use those services. Women in some contexts may be less likely to have cash to be able to pay for a coffee in a cafe that also offers access, or it may not be safe for them to carry it. In some contexts, due to cultural or security factors, going to a public space, particularly alone, might not be so possible for women. In Ethiopia there was a famous photo that captured this well. It was of people leaning against a university wall checking their mobile phones for an internet connection during a shutdown—all men.[46]

Data Breaches

Data breaches have become commonplace and can occur for a number of reasons, as a result of cybercriminals looking to make a profit, cyberespionage to gather intelligence, or cyber-blackmail to coerce desired behavior. Data breaches can also result from hacking by foreign powers which can be seen as an intentionally wrongful act in cyberspace. While attribution of such attacks is difficult, China's hacking of a United States' Navy contractor in which "massive amounts of highly sensitive data related to undersea warfare" were stolen, is one example.[47] Data collection never takes place in a gender-neutral setting, so when data breaches occur, even if they are not targeting people specifically on the basis of gender, they can have a more severe impact on women and LGBTIQ people because of historical and structural inequalities in power relations based on gender and sexuality. This subsection explores data breaches that did not take place in the context of international conflict in cyberspace due to a lack of available information on those that have, but nonetheless illustrate how data breaches can have a gendered impact.

For example, in July 2016, the municipality of São Paulo experienced a data breach exposing the personal data of an estimated 650,000 patients from the Brazilian public health system. This massive data breach included names, addresses, and medical information such as information about pregnancy and abortion care.[48] According to the media, the personal data was from 2001 to 2007 and referred – in almost all of the cases – to women at some point of their pregnancy. Among those affected were 15,926 mothers who had given birth before seven months of gestation, 4,237 abortions and 181 recent stillbirths. It is worth noting that abortion is illegal in Brazil, so this data breach not only violated the right to privacy of the women affected around a socially sensitive issue, but also exposed them and their doctors to potential criminal charges.

The aforementioned example constitutes a clear example that personal data breaches can dramatically affect not only women's privacy but also their sexual and reproductive health rights, their dignity and self-development. When data breaches occur it is crucial to observe with a gender lens which human rights can be affected and analyse it beyond only a consideration of privacy rights; in this case, a hospital is a critical infrastructure (because of the management of sensitive and health data) that should have heavy security measures as part of a cyber security policy respectful of human rights. This highlights a key point, the need for countries to implement cyber security policies with a human rights perspective.

Another massive data breach occurred in Chile in 2016. In this case, a public hospital suffered a cyber security failure and made available to their workers and even to the general public (via their intranet) more than three million health records including the names, ID numbers, and addresses of women and girls who asked for the morning-after pill in a public hospital and people living with HIV.[49] The authorities had been alerted to this flaw in the hospital's computer system 10 months earlier, but neither the authorities nor the company in charge of

[46] Interview with Berhan Taye, Senior Policy Analyst, Access Now, 10 February 2020.

[47] Ellen Nakashima and Paul Sonne, "China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare", *The Washington Post,* 8 June 2018, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html

[48] R. Hernandes, "Gestão Haddad expõe na internet dados de pacientes da rede pública", Folha de Sao Paulo, 6 July 2016, https://www1.folha.uol.com.br/cotidiano/2016/07/1788979-gestao-haddad-expoe-na-internet-dados-de-pacientes-da-rede-publica.shtml

[49] M. Jara and V. Carvajal, "Grave falla en la red del Minsal dejó expuesta información confidencial de pacientes," CIPER, 3 March 2016, https://ciperchile.cl/2016/03/05/grave-falla-en-la-red-del-minsal-dejo-expuesta-informacion-confidencial-de-pacientes

the hospital's cyber security took action to remedy the situation despite being warned of the risks.[50] The people most affected by the data breach were women, girls, and people living with HIV. Women and sexual minorities are more profoundly affected by the consequences of these kinds of data breaches because they may face discrimination or even prosecution as a result. These breaches impact not only their right to privacy but also their sexual and reproductive health and rights.

Disinformation

Disinformation campaigns involve the deliberate sharing and spreading of false information in order to achieve a desired goal or influence a situation. While political propaganda has existed for centuries, modern disinformation campaigns utilise ICTs, especially social media platforms, in any number of ways: the use of 'political bots' to amplify hate speech or tensions; placing manipulated content to sway opinion; exploiting data about users for micro-targeting; or deploying an army of trolls to harass political candidates, leaders, dissidents, journalists, or ordinary people expressing a political opinion online.[51] As the internet and social media have become primary platforms for information sharing, news, and political campaigning in many countries because of the ease with which people can connect through them, that same easy access—and anonymity—can transform those platforms into arenas of abuse, humiliation, and used to discredit, often on the basis of false information. Traditionally seen as a human rights issue, as it pertains to content, disinformation is rapidly becoming a matter for global security when states use disinformation campaigns to influence events in another country or target foreign nationals.

Research shows that there is a strong gender dimension in politically motivated disinformation activities.[52] As gender identity and sexual orientation are identifiers, they can become the basis on which someone is targeted to receive information across platforms. Doing so makes certain gendered assumptions about one's interests and ability to be influenced.

Gender norms also play a large role in direct attacks of false information. Women are already significantly under-represented in global media coverage of political issues[53] and stories of female politicians and candidates often reinforce highly gendered stereotypes and norms by focusing on the way women are dressed, their body image, and their family life, with much less attention paid to their ideas, policies and proposals.[54] Disinformation activities perpetuate these trends and often in more malicious ways. Ahead of parliamentary elections in Georgia in 2016, for example, several female politicians were targeted by fake videos meant to depict them engaging in sexual activities, and in one case, an extramarital affair. The men implicated in the latter example were not impacted because male adultery is socially acceptable—except for one man who was labelled by media as gay, which put him at risk due to strong homophobia in the country.[55]

In 2018, a shadowy video and blurry screenshots of a naked woman straddling a man was published in the Philippines and were claimed to be Leila de Lima, a senator and strong critic of president Duterte. It was never proven to be her in the video but it damaged her reputation and eroded her support base, which may have made a subsequent political move against her easier.[56]

A woman Al-Jazeera reporter in the Philippines was the target of false stories asserting that she had undergone plastic surgery. A meme was circulated that placed her face beside that of another journalist, with the caption,

[50] Ibid.

[51] Samantha Bradshaw and Philip N. Howard, The Global Disinformation Disorder: 2019 *Global Inventory of Organised Social Media Manipulation,* Working Paper 2019, Oxford, UK, Project on Computational Propaganda.

[52] This report is focusing on women more than other vulnerable or marginalised groups but encourages further research into the differentiated impact of disinformation campaigns on the basis of gender more broadly.

[53] See Global Media Monitoring Project, 2015.

[54] Lucina De Meco, *#Shepersisted: Women, Politics & Power In The New Media World,* Fall 2019, p. 10.

[55] Nina Jancowicz, "How Disinformation Became a New Threat to Women," 11 December 2017, https://codastory.com/disinformation/how-disinformation-became-a-new-threat-to-women/

[56] P. Occeñola, "Fake News Real Women: Disinformation gone macho", 15 December 2018, https://www.rappler.com/newsbreak/in-depth/217563-disinformation-gone-machao

"When the looks God gave you simply isn't enough".[57] The head of a non-governmental organization there explains that male journalists are also attacked "…but when it is a female journalist, it centers on their being a woman, on their bodies, like, 'you're so ugly, but I still hope you get raped.'"

A recent Inter-Parliamentary Union (IPU) survey of 55 women legislators worldwide found that 81.8 percent of the respondents had experienced psychological online gender-based violence, including high incidences of humiliating or sexual images having been circulated, where were often fake or doctored.[58] Tracking in the United States shows that female politicians there are often the target of online abuse and this is a particular problem for women of colour.[59]

Women politicians or other leaders are targeted more often than their male counterparts are; for example, Hillary Clinton received twice as many tweets containing insults and offensive comments as Bernie Sanders during their campaigns for the United States' Democratic Party nomination. The same was true of Julia Gillard in comparison to Kevin Rudd between January 2010 and January 2014, in Australia.[60]

Not all of these activities can be strictly considered as "disinformation", although it could be argued that they should not be discounted either: a high incidence of abuse, with or without an information base, can still serve to deter or discredit. Where disinformation campaign activities influence events in another country, or target foreign nationals, it becomes relevant to international cyber security.

These examples are fewer and suffer from the same attribution challenges as any cyber operation but they do exist. A recent Oxford University report on disinformation notes that the release of limited information about "foreign influence operations" from Twitter and Facebook shows that a small but sophisticated group of countries are engaging in disinformation activities.[61] A Bellingcat researcher revealed in 2019 a disinformation campaign in which Saudi Arabia created more than 300 Facebook accounts and pages masquerading as local news organizations in countries throughout the Middle East and North Africa, in the wake of the death of Jamal Khashoggi.[62] The pages, which were eventually removed by Facebook, posted content praising Crown Prince Mohammed bin Salman, the presumed mastermind behind Khashoggi's death, or targeting enemies of Saudi Arabia, including Amnesty International, Al Jazeera, or countries like Iran. While Russian efforts to meddle in the 2016 US elections through disinformation (and other means) is now common knowledge, what is less known is that as far back as 2014, Russian propaganda operations conducted a dry run, impersonating social media accounts of black feminists in the US in order to gain support among their supporters.[63] In fact, black feminists documented fake accounts, misinformation, bot networks, and weaponized trolls using the hashtag #YourSlipIsShowing.[64] In 2018, a New Knowledge report[65] commissioned by the US Senate described how Russian agents specifically "focused on developing black audiences and recruiting black Americans as assets," but never picked up on the gender dimension of the propaganda operation, or credited the black feminists who documented it.

[57] M. Buster, "Busted: Al Jazeera reporter hits Duterte supporter for claiming she had cosmetic surgery, using a different woman's photo", 20 April, 2017, https://memebuster.net/al-jazeera-reporter-hits-duterte-supporter/

[58] Inter-Parliamentary Union, *Sexism, harassment and violence against women parliamentarians,* October 2016, http://archive.ipu.org/pdf/publications/issuesbrief-e.pdf

[59] M. Astor, "For Female Candidates, Harassment and Threats Come Every Day" 24 August 2018, https://www.nytimes.com/2018/08/24/us/politics/women-harassment-elections.html

[60] E. Hunt, N. Evershed and R. Liu, "From Julia Gillard to Hillary Clinton: online abuse of politicians around the world," *The Guardian,* 27 June 2016. www. theguardian.com/technology/datablog/ng-interactive/2016/jun/27/from-juliagillard-to-hillary-clinton-online-abuse-of-politicians-around-the-world

[61] China, India, Iran, Pakistan, Russia, Saudi Arabia, and Venezuela. See Bradshaw and Howard, p. 2.

[62] See "Inside Saudi Arabia's Disinformation Campaign", *NPR,* 10 August 2019, https://www.npr.org/2019/08/10/750086287/inside-saudi-arabias-disinformation-campaign

[63] R. Hampton, "The Black Feminists Who Saw the Alt-Right Threat Coming", 23 April, 2019, https://slate.com/technology/2019/04/black-feminists-alt-right-twitter-gamergate.html

[64] "Your slip is showing" in the Southern black dialect of South Florida refers to something that's meant to be concealed but is, embarrassingly, on full display.

[65] S. Shane and Sheera Frankel, "Russian 2016 Influence Operation Targeted African-Americans on Social Media", *New York Times,* 17 December 2018, https://www.nytimes.com/2018/12/17/us/politics/russia-2016-influence-campaign.html

A Finnish journalist who exposed a fake news operation and troll farm in St. Petersburg was later the target of stories from Russian media outlets alleging that she had engaged in drug use and sales.[66] In the run-up to the 2019 Indonesian elections, Grace Natalie, head of the Indonesian Solidarity Party (PSI), was accused by an anonymous Twitter user of having an extra-marital affair with Pak Ahok, the former governor of Jakarta. The accuser claimed to have access to a sex tape, which they threatened to make public. She challenged him to release it and he did not, which vindicated her, but some speculated that had even a fake video been produced it could have influenced the election. The growth of "deep fakes" are becoming a complicating factor and a new tactic, making it more difficult to distinguish between what is real and what is false.[67]

Section IV: Participation

The 'gender digital divide' is real. As already outlined in this report, there is a substantial, and in some cases growing, divide between women and men in their access to and use of the internet.

Beyond issues of access, there is another dimension of this divide that warrants attention—the gender gap in participation within all aspects of the cyber security field. This gap has been well-established within relevant technological and business sectors. For example, while precise estimates vary, most surveys place women's participation levels in all ICT-related professions at between 15-20 percent, and slightly lower for information security.[68] The World Economic Forum's Gender Gap report notes that only 22 percent of artificial intelligence (AI) professionals globally are female, compared to 78 percent who are male.[69] This is not only problematic in the context of gender parity, but also because it means that technology, which always reflects the values and biases of its developers, will further entrench problematic gender norms and stereotyping.[70] Multiple studies and testimonies highlight how entrenched gender biases and stereotypes are steering girls and women away from science and related fields. Even in countries that score higher in gender equality indexes, this remains a problem.

What has been less examined is the participation of women working in cyber security policy and diplomacy, including confidence and capacity-building measures, whether at national, regional, or international levels. This section will seek to identify gender participation gaps in international and regional cyber security fora, the causes and consequences of such gaps, and practical steps to help address them. Due to the constraints outlined in the introduction, this research is focused primarily on women's participation, although the researchers highlight the necessity of diversity and an intersectional approach. Five interviews were done with women in mid-career to senior positions in national governments, or regional and international organizations, where their role focuses on cyber security in a non-technical way. They were selected for their experience and to ensure regional diversity. Researchers reached out to a further four women for interviews but they were unavailable.

[66] Jessikka Aro, "How pro-Russian trolls tried to destroy me", *BBC,* 6 October 2017, https://www.bbc.com/news/blogs-trending-41499789

[67] 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/

[68] See J. Reed, Y. Zhong, L. Terwoerds and J. Brocaglia, *The 2017 Global Information Security Workforce Study: Women in Cybersecurity,* https://iamcybersafe.org/wp-content/uploads/2017/03/WomensReport.pdf and (ISC)2, The 2013 (ISC)2 Global Information Security Workforce Study, https://www.isc2.org/giswsrsa2013/

[69] World Economic Forum, "Assessing Gender Gaps in Artificial Intelligence", *Global Gender Gap Index 2018,* http://reports.weforum.org/global-gender-gap-report-2018/assessing-gender-gaps-in-artificial-intelligence/

[70] Mahita Gajana, "AI Voice Assistants Reinforce Gender Biases, U.N. Report Says," *Time Magazine,* 22 May 2019, https://time.com/5593436/ai-voice-assistants-gender-bias/

But Why Diversity?

The rationale for improved women's participation, and gender diversity more broadly, is rooted in a simple premise: cyber security is an issue that impacts everyone, and women are stakeholders who should have equal opportunities to participate in the decisions, policies, and programs that will affect them. Their inclusion expands the diversity of perspectives and skills available, thereby contributing to overall effectiveness and sustainability. In particular, as the previous section demonstrated, women face different threats in the context of cyber security, and may bring different threat models and priorities to discussions.

Most research on the specific benefits of gender diversity, or of women, in cyber security come from the private sector and often stresses the "soft skills" that women tend to emphasize in their resumes, such as interpersonal and analytical skills, as well as the "business case" for hiring more women.[71] While this analysis reinforces various gender stereotypes of 'womanly characteristics', it does highlight skill sets that are equally critical for cyber security policy or diplomacy work, such as in the area of confidence-building measures, negotiation, or incident response and coordination.

More is known however about the benefits of women's direct participation in peace negotiations for the longevity and success of related agreements. A study investigating 82 peace agreements in 42 armed conflicts between 1989 and 2011 found that peace agreements with women signatories are associated with durable peace.[72]

Research also shows that women's participation in a negotiation process is more likely to lead to the inclusion of gender provisions; an analysis of 98 peace agreements across 55 countries between 2000 and 2016 found that peace agreements are more likely to have gender provisions when women participate in track 1 or 2 peace processes.[73] It can be inferred then that in order for cyber security policy and diplomacy to reach outcomes that account for the experiences and needs of women, their participation is a necessity—as stakeholders, but also as advocates for themselves.

Security—An Old Boy's Club

It is challenging to paint a statistically precise picture of the current status of women's participation in these aspects of the cyber security field for two reasons: first, the fields themselves are indistinct and individuals may play many roles, such as being involved in national implementation of globally agreed norms, to attending multilateral negotiations. The second reason is that there has not been wide-ranging tracking of gender- or sex-disaggregated participation rates.

> ***In Focus – Gender report cards***
>
> *Recognizing the absence of consistent and reliable gender-disaggregated data on participation in internet governance spaces, starting in 2011 theWomen's Rights Programme of the Association for Progressive Communications (APC) began compiling Gender Report Cards to monitor and assess the level of gender parity and inclusion at the UN Internet Governance Forum (IGF).*[74] *These Gender Report Cards have been instrumental in monitoring the level of gender parity and inclusion at IGF workshop sessions. Efforts by the IGF Dynamic Coalition on Gender made reporting on gender diversity in IGF workshops part of the official reporting process, which transformed this from a civil society initiative into a formal part of the Forum's work . In 2015, the IGF Secretariat published the first overall analysis of gender participation in the IGF, based on gender report cards.*[75]

[71] Fortinet, Exploring the Benefits of Gender Diversity in Cybersecurity", 4 October 2018, https://www.fortinet.com/blog/business-and-technology/exploring-benefits-gender-diversity-cybersecurity.html

[72] Krause, J. Krause, W & Bränfors, P., "Women's Participation in Peace Negotiations and the Durability of Peace", *International Interactions,* 44:6, pp. 985-1016.

[73] Jaqui True and Yolanda Riveros-Morales, "Towards inclusive peace: Analysing gender-sensitive peace agreements 2000-2016", *International Political Science Review,* 27 November 2017.

[74] The report cards and relevant background information can be found at https://www.genderit.org/feminist-talk/igf-gender-report-cards

[75] "Joao Pessoa, "Gender report cards: Analysis and results", November 2015, https://www.intgovforum.org/cms/documents/igf-meeting/igf-2016/takingstock/726-gender-report-card/file

A useful starting point can be official meeting and participation records from relevant meetings or events. An overview of gender diversity and women's participation in United Nations processes on cyber security in the context of international security by the UN Institute for Disarmament Research (UNIDIR)[76] reveals strong and consistent gender imbalance:

- In the six UN GGEs that have been convened in the last 15 years, women have represented on average only 20.2 percent of participants.
- As recently as the fifth GGE, convened in 2016-2017, women represented only 20 percent of participants.
- The current and sixth GGE, being convened in 2020-2021, does have gender parity, which is credited to the UN Secretary-General's commitment to achieving gender parity "in all panels, boards, and expert groups established under his auspices in the field of disarmament" as contained in Action 37 of his 2018 Agenda for Disarmament.[77]
- At the first session of the UN Open-Ended Working Group (OEWG) on Developments in the Field of Information and Telecommunications in the Context of International Security in September 2019, 32 percent of 414 participants were women and 68 percent were men; while only 24 percent of delegations were led by women.
- At the second session of the OEWG in February 2020, there were a total of 148 women (39%) and 233 men (61%). This includes non-member state delegations such as the Holy See, the European Union, and the International Telecommunication Agencies. At the second session, 34 of the 114 delegations included no women and 10 delegations had no men.[78]
- One hundred and nineteen statements, out of 280 total statements delivered during the second substantive OEWG session in February 2020, were delivered by women delegates.[79]

These numbers are consistent with what has been observed in other UN forums that cover matters of disarmament, non-proliferation, or arms control, which is where both of the UN cyber processes have their basis.[80] Interestingly, research shows that the gender gap is greatest in UN bodies on this issue area—the UNGA Third Committee (on social, humanitarian and cultural issues) has the highest proportion of women representatives attending, at 49 per cent in 2017, in contrast to the First Committee on disarmament which has the lowest.[81] This may speak to the perceived dichotomy between the issues covered by those committees, the "feminization" of different disciplines, and how people are encouraged to engage with one or the other onthe basis of their gender.[82]

Looking beyond the UN cyber security forums, the gap exists in other policy bodies. As one example, when INTERPOL countries were requested to provide participation statistics to Monitoring and Assessment missions on cybercrime, none were able to provide gender dis-aggregated statistics.

Recognizing the need to promote gender equality in its own work, the International Telecommunication Union adopted a resolution at its 2018 Plenipotentiary meeting committing member states and sector members (typically private sector entities from the ICT sector) to take a number of actions, including to encourage gender-balanced

[76] "Factsheet—Gender in Cyber Diplomacy", UN Institute for Disarmament Research, https://www.unidir.org/publication/fact-sheet-gender-cyber-diplomacy

[77] Antonio Guterres, *Securing our Common Future: An Agenda for Disarmament,* May 2018, https://www.un.org/disarmament/publications/more/securing-our-common-future/

[78] Analysis of participant data by the Gender Team of the UN Office for Disarmament Affairs. Reasons for noticeable increase in gender diverse participation are explained later in this report.

[79] Allison Pytlak, "A new 'Women In Cyber' fellowship has a big impact on the OEWG", *Cyber Peace & Security Monitor: Volume 01, Number 07*, 18 February 2020 http://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.7.pdf

[80] Both the GGE and the OEWG were established by resolutions adopted by UN member states at the 2018 session of the UN General Assembly First Committee on Disarmament and International Security.

[81] Renata Hessmann Dalaqua, Kjølv Egeland, Torbjørn Graff Hugo, *Still Behind the Curve,* UNIDIR, p. 19, https://www.unidir.org/publication/still-behind-curve

[82] Ibid., p.33.

representation in delegations to ITU conferences, assemblies and other meetings, as well as in candidatures for leadership roles. It also resolved the ITU itself to compile and process statistical data from countries and draw up indicators that take into account gender equality issues and highlight trends in the sector, disaggregated by socio-economic factors, in particular sex and age and to take affirmative measures when necessary, in ITU as a whole, to ensure capacity building and the appointment of women to senior-level positions, including ITU elected positions.[83]

When looking at participation rates, it's important to look beyond numbers alone. Are women able to contribute in ways that are meaningful? What specific roles do they fill, what leadership and decision-making roles do they hold, and are their skills and inputs valued? The same UNIDIR report shows that in arms control, non-proliferation and disarmament forums, heads of delegations are mostly men and the proportion of women tends to decline as the importance of the position increases, while the proportion of men grows linearly as one moves "from regular diplomatic personnel to United Nations ambassadors, to foreign ministers and, lastly, to heads of State or Government."[84]

Moreover, numbers do not give a sense of the discrimination that women experience, or the social and cultural gender dynamics that persist in their working environments. In the course of preparing this report, all five women interviewed stressed the invisible gender discrimination they have encountered as a result of working in a heavily male-dominated field, or how that has set a tone and dynamics for the environment they work in.

"When you are in a room with many men, the social norms tend to be masculine. The socialization makes the structure," noted one interviewee. Another interviewee described a situation that occurred earlier in her career in the context of having an older male colleague who reported to her. She explained that people regularly assumed that she reported to him, as evidenced that he was invited to principal-level meetings in her place. Another interviewee said that sometimes when she attends meetings with her junior male colleague other people assume the male is the boss.

Three interviewees described how they have had to adapt their behaviour in various ways to better 'succeed' in male dominated spaces, such as through gender assertiveness training. "We have to claim our place," said one interviewee, explaining that she always deliberately raises her hand or national flag in a meeting to ask questions, deliver a response, or similar just to make the point that she is in the room and has a voice. She observed that women often feel that "we need to know things 110 percent before [we feel] are really an expert" whereas men hesitate less to give an opinion; an observation that was supported by another interviewee.

Barriers and Challenges

The reasons underpinning the gender gap in these aspects of cyber security are multiple, and often, context specific.

In many instances however, the gap goes back to unequal access and/or a lack of encouragement to engage in the cyber security field, in any capacity, as already described. As one interviewee highlighted, "In many regions the issue of access in many mainstream professions are systemic, and for digital related fields it can be compounded with the sheer lack of access to online resources."

This is rooted in the prevailing patriarchal and masculine structures on which most societies are based, in which women do not associate themselves with work in a security profession.[85] A complicating factor is that, as this report has already revealed, women are often the targets of online GBV and abuse, which reinforces a sense of being targeted and unwelcome. Yet, if more women were to work within cyber security and in leadership roles, these perceptions could be reversed and solutions and structures that work for women developed.

[83] ITU Plenipotentiary Resolution 70, "Mainstreaming a gender perspective in ITU and promotion of gender equality and the empowerment of women through telecommunications/information and communication technologies", 2018, https://www.itu.int/en/ITU-D/Digital-Inclusion/Documents/Resolutions/RESOLUTION%2070%20(REV.%20DUBAI,%202018).pdf. See Annex I for more details on the commitments by states included in ITU Resolution 70

[84] Ibid., p.6.

[85] Donna Peacock and Alastair Irons, "Gender Inequalities in Cybersecurity: Exploring the Gender Gap in Opportunities and Progression," *International Journal of Gender, Science and Technology,* Vol.9, No.1, 2018, p. 26.

The women interviewed all indicated that they personally did not face many formal obstacles or barriers to working in their field and receiving relevant training and education. Their combined backgrounds include legal, political science, and molecular biology degrees alongside experience in compliance, global trade, and knowledge of coding and computer science. Yet most described situations where either they, or another female colleague, were not taken seriously despite relevant expertise or being in a leadership role. While it was hard for them to specify that this was on account of their being a woman, they felt that it did relate to assumptions and gender norms. One described that she has sometimes deliberately asked a male colleague to reiterate her points in a negotiation or meeting room, after feeling that she was not being heard.

Two interviewees also highlighted that negative gender dynamics can become something that cause women to leave the profession. This points to another important consideration: how women's participation in other professions is being impacted by disinformation campaigns and online GBV, as described in Section II.. "All it takes is a fake story and smear campaign fabricated by a journalist to ruin years of hard work," says Joyce Banda, the former president of Malawi in a new report on women and media. "This makes women nervous to run for office, because not only can it harm her political aspirations, but also bring shame to her family."[86] Other women surveyed for the same report expressed similar concerns; most reported being "extremely concerned about the pervasiveness of gender-based abuse (ranging from insults to death threats) in the digital space as a real barrier for women who want to engage in politics."[87]

Gender norms in relation to parenting and family life can also be a factor, although this is probably true of most professions and not unique to cyber security. One interview said that this may be more of a barrier in diplomacy than "cyber", in which all of the women she knows in her Ministry are divorced and single, and those who are not have partners willing to follow them as they move to new postings. She further described stigmatization against women with families, with single people being perceived as being able to work more, and therefore able to become more successful.

How to Support Women's Participation in Cybersecurity Diplomacy

The key to involving more women in cyber security in ways that drive change and influence policy outcomes towards greater peace and stability is to look beyond "adding women" in a tokenistic way and to make it meaningful. This requires addressing the underlying gender norms that act as barriers and disincentives, as well as investing in knowledge-sharing and network-building. As one interviewee stated, "The big mistake that we make often is to think that the numbers are the only thing that matters." Another added, "I think tackling [access] at the granular level to resolve the access issue will build a cadre of women who are more knowledgeable and can take part in more meaningful discussion."

At the national level, resources allocated to address gender equality are consistently low, sometimes less than one percent of national budgets.[88] But more positively, there are multiple initiatives underway within international bodies, supplemented by guidelines, agreements, and crucially, resourcing.

In the context of the UN's OEWG on cyber security, for example, five governments have initiated a fellowship program for around 25 women working within cyber security in their national governments, from the regions of Africa, Asia, Latin America and the Caribbean, and the Pacific. The program includes knowledge-building opportunities on thematic topics as well as negotiating skills, after which they participate in the OEWG substantive session with their national delegation. Participation of the fellows went a long way toward closing the gender gap during the OEWG's second session in February 2020 and also increased the level of technical expertise in the room.

The momentum within these bodies is possibly buoyed along by a broader swell of support for inclusion of gender perspectives within disarmament and arms control. Many treaties or instruments are being re-interpreted in "gender-sensitive ways" such as through a new emphasis on improving gender- and sex-disaggregated information, gender-based violence preventing in relation to armed violence, and increasing gender diversity. During the 2019 UNGA First Committee session, an unprecedented 28 per cent of all adopted 2019 resolutions include gender aspects.[89] There could be lessons and examples here for the cyber security community.

[86] De Meca, p. 11.

[87] Ibid., 30.

[88] OAS (2017). Third Hemispheric Report on the Implementation of the Belém do Pará Convention.

[89] Katrin Geyer, "Gender", *First Committee Monitor,* November, 2019, http://reachingcriticalwill.org/images/documents/Disarmament-fora/1com/FCM19/FCM-2019-No6.pdf

The Organization of American States (OAS) has started implementing initiatives to raise awareness about the importance of cyber security policies that are gender sensitive. It encourages member states to nominate a more gender-balanced delegation to its activities and provide incentives to facilitate women's participation whenever possible. At the same time, it also works to encourage its member states to include provisions to promote equal access to science and technology education and professions for women in order.[90] Many OAS states run a "CyberWomen Challenge" in partnership with tech company TrendMicro and partnership with countries like Canada and the United Kingdom, which is focused on developing cyber security skills in women in the ICT industry throughout Latin America to help bridge the diversity and skills gap. In 2018, more than 650 women participated in the trainings.[91] It is part of a collaboration agreement between organizations to promote initiatives that contribute to a more secure and inclusive insurance in the field of cyber security.[92] Additionally, OAS states are bound by the Inter-American Program on Women's Human Rights and Gender Equity and Equality (IAP), adopted in 2000, which one interviewee pointed to as acting as a baseline for improving participation in cyber security.[93]

There are a growing number of tools and guidelines to draw on, such as the frameworks and agendas outlined in Annex I. Additional resources include: the Government of Canada's *Playbook for Gender Equality in the Digital Age;*[94] *Securing our Common Future: An Agenda for Disarmament;*[95] and the UN's Guidelines for Gender Inclusive Language.[96]

Finally, most interviewees spoke to the importance of mentorship and support networks in their own experience.

In any initiative, it will be important to avoid gender essentialisms, and understand that women's participation is rooted in a broader need for diversity. It is important that participation not be co-opted to support other agendas or the further militarization of cyberspace, and that efforts to build capacity are not, even unintentionally, presented in ways that can be viewed as patronizing or undermining of the experiences and knowledges that any woman already brings to the table. The problem of gender diversity is not a "cyber" problem, but a broader societal one which manifests as gender inequality in cyber security spaces. To address this, broader changes in the overall culture is vital.

[90] Email correspondence with Government of Canada, Anti-Crime Capacity Building Program, February 2020.

[91] Ibid.

[92] Ibid.

[93] Ibid.

[94] Digital Inclusion Lab, *Playbook for Gender Equality in the Digital Age,* Government of Canada, 2018, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/human_rights-droits_homme/playbook-manuel_instructions.aspx?lang=eng

[95] Antonio Guterres, Securing our Common Future: An Agenda for Disarmament, May 2018, thttps://www.un.org/disarmament/publications/more/securing-our-common-future/

[96] United Nations, Guidelines for Gender Inclusive Language, https://www.un.org/en/gender-inclusive-language/guidelines.shtml

Section V: Recommendations

Based on the information presented in this report, the researchers put forward the following recommendations:

Normative and structural recommendations:

- States should integrate their obligations to protect, promote and uphold women's human rights as part of their cyber security strategies;
- States should utilize WPS National Action Plans or opportunities provided by other frameworks to advance women's participation within international cyber security, alongside their protection; and
- States should conduct a gender audit of national or regional cyber security policies to identify areas for improvement.

Recommendations relating to impact and cyber security operations:

- States and companies should adopt data minimization as a key principle of data protection, to minimize the risk experienced by women, when data breaches (inevitably) occur;
- All actors involved in cyber incident response (governmental, private sector, and civil society) should be equipped to recognize potential gendered impacts of an operation and respond appropriately, as well as conduct further research into those impacts to improve global understanding and knowledge;
- All actors should call out and condemn online gender-based violence, whether in the context of disinformation activities or otherwise, and draw on and support research done by women, especially minority women, who are best placed to document online GBV; and
- Provide media or digital security training to reduce the personal and professional impacts of online disinformation campaigns, and other forms of online GBV.

Recommendations relating to participation:

- All actors should maintain sex- or gender-disaggregated participation records for all cyber security related work (diplomacy, capacity building, incident response, etc.);
- All actors should build intentionally supportive and inclusive spaces and work cultures in the cyber security policy/diplomacy field that will encourage and act as incentive for greater diversity in participation; and
- States and private companies should allocate resources for further research and knowledge-sharing/capacity-building on the gender dimensions of international cyber security, as well as for programs and initiatives that actively seek to reduce gender inequality.

Recommendations related to the UN's OEWG on ICTs:

- States should specifically acknowledge their obligations to uphold women's rights online, in the context of recognizing the applicability of international human rights law, because of the differential threats they experience due to cyber incidents;
- States should recognize that, as part of the threat landscape, international cyber operations can have gender-differentiated impacts;
- States should encourage further analysis or promotion of the eleven voluntary norms include a gender dimension;
- States should recognize that capacity-building must be gender-sensitive and gender diverse;
- States should commit to gender diversity in delegations to meetings and inclusive approaches to developing positions, statements, or other contributions.

Annex I: Normative Frameworks Relevant to Gender and Cyber Security

The Women, Peace and Security (WPS) Agenda

- The WPS Agenda was established by UN Security Council Resolution (UNSCR) 1325[97] in 2000 and was considered a milestone achievement that emerged from years of advocacy from women-led civil society.[98] It was the first time that the Security Council recognized and addressed the disproportionate impact of armed conflict on women—while also stressing the importance of women's equal and full participation as active agents in peace and security. In doing so it moved beyond framing women solely as victims or a vulnerable group.
- The WPS Agenda is best understood as a set of approaches jointly rooted in the principle that 'effective incorporation of gender perspectives and women's rights can have a meaningful and positive impact on the lives of women, men, girls, and boys on the ground.' [99]
- The WPS Agenda is generally understood to have four pillars: participation, prevention protection, and relief and recovery. The first three are referred to as the 'three Ps'.
- Nine 'follow-up' WPS resolutions have been adopted by the Security Council, which variously address sexual violence in conflict, the role of women in peace processes, resourcing, among other things.[100]
- National Action Plans (NAPs) are a primary vehicle for the implementation and localization of UNSCR 1325 commitments.[101] They are meant to outline a member state's domestic and foreign policy actions undertaken to meet the WPS objectives and are envisioned as a critical way to ensure compliance with the provisions of the resolutions. Yet less than half of UN member states have established a NAP, and implementation those that do exist is uneven, often because of a lack of designated resources.
- There has been insufficient examination of how the WPS Agenda or NAPS could be integrated or leveraged within policy discussions on international cyber security. Given the legally binding nature of UNSCR resolutions on all UN member states, it could serve as a foundation for efforts to close the gender digital divide and prevent better protections online.

Beijing Declaration and Platform for Action[102]

- The Beijing Declaration and Platform for Action was agreed by states during the Fourth World Conference on Women in 1995. Considered by many to be a groundbreaking and historic achievement to advance women's rights and participation, it was negotiated with significant input from civil society and still enjoys wide-ranging support.
- The Platform for Action is organized across 12 areas of concern and is balanced between calls to enhance women's participation and recognizing the unique needs and experiences of women.
- It is highly critical of excessive military spending and armament, noting that "that those affected most negatively by conflict and excessive military spending are people living in poverty, who are deprived because of the lack of investment in basic services." Strategic Objective E.2 outlines multiple actions to reduce excessive military expenditures and control the availability of armaments.

[97] United Nations Security Council, *Women and peace and security,* S/RES/1325, 31 October 2000, http://unscr.com/en/resolutions/1325

[98] PeaceWomen, Background, https://www.peacewomen.org/why-WPS/solutions/background

[99] PeaceWomen, "UN Security Council Resolution 1325", https://www.peacewomen.org/SCR-1325

[100] Highlights of each resolution and links to the resolutions can be found at https://www.peacewomen.org/security-council/WPS-in-SC-Council

[101] The PeaceWomen program of the Women's International League for Peace and Freedom tracks the development and implementation of WPS National Action Plans. See https://www.peacewomen.org/who-implements

[102] *Beijing Declaration and Platform for Action,* 15 September 1995, https://www.un.org/womenwatch/daw/beijing/pdf/BDPfA%20E.pdf

- Section J of the Beijing Platform[103] addresses women and the media, including new communication technologies. Specifically, it recognizes that "During the past decade, advances in information technology have facilitated a global communications network that transcends national boundaries and has an impact on public policy, private attitudes and behaviour, especially of children and young adults. Everywhere the potential exists for the media to make a far greater contribution to the advancement of women." It also recognizes that the continued projection of negative, violent, and degrading images of women in media communications, including electronic media negatively affect women and their participation in society while also reinforcing their traditional roles.
- Section J calls for women to be involved in decision-making regarding the development of the new technologies in order to participate fully in their growth and impact, and includes a strategic objective to this end (Strategic objective J.1.).

Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW)[104]

- CEDAW was adopted by the United Nations General Assembly in 1971 following three decades of work by the United Nations Commission on the Status of Women and is sometimes described as a "bill of rights for women". As of 2020, there are 189 states parties.
- The preamble acknowledges that "extensive discrimination against women continues to exist" and emphasizes that such discrimination "violates the principles of equality of rights and respect for human dignity". The remainder of the Convention outlines an agenda for equality across three thematic areas.
- Implementation of states parties obligations is monitored by the CEDAW Committee. States parties are obligated to submit a report every four years, which are discussed during an annual session. The CEDAW Committee can also publish general recommendations, which serve as authoritative interpretations articles of the Convention. In recent years general recommendations have taken into account ICTs.
- The CEDAW Committee's General Recommendation No, 35 on " gender-based violence against women" [105] includes in its updated understanding of gender-based violence against women the "redefinition through technology-mediated environments, such as contemporary forms of violence occurring in the Internet and digital space".
- The CEDAW Committee's General recommendation No. 36 "on the right of girls and women to education" [106] recognizes the underrepresentation of women "in the use of Information Communication Technology (ICT) skills" and further calls on schools to address the barriers that impede access to information and employment opportunities in relevant industries.

The 2030 Agenda[107]

- The 2030 Agenda is a broad and interdependent approach to sustainable socio-economic development that builds on earlier multilateral processes and agreements.
- The 17 Sustainable Development Goals (SDGs) are the primary mechanisms of the 2030 Agenda, adopted by the UN General Assembly in resolution A/RES/70/1 'Transforming our world: the 2030 Agenda for Sustainable Development' (UNGA, 2015) amid strong political support and commitment.
- SDG 5 seeks to "Achieve gender equality and empower all women and girls". Like all of the Goals, SDG 5 has a set of specific targets and corresponding indicators, some of which are especially relevant:

  » 5.1: End all forms of discrimination against all women and girls everywhere.
  » 5.2: Eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation.

[103] Strategic Objective J.1, https://www.un.org/womenwatch/daw/beijing/platform/media.htm

[104] To access an overview of the Convention, as well as its text, status of implementation, number of states parties and other updates visit https://www.un.org/womenwatch/daw/cedaw/

[105] Committee on the Elimination of Discrimination Against Women, *General recommendation No. 35 on gender-based violence against women, updating general recommendation* No. 19, 14 July 2017, https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/1_Global/CEDAW_C_GC_35_8267_E.pdf

[106] Ibid, paragraph 24.

[107] Sustainable Development Goals Knowledge Platform, https://sustainabledevelopment.un.org/

- » 5.5: Ensure women's full and effective participation and equal opportunities for leadership at all levels of decision-making in political, economic and public life.
- » 5.B: Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women.[108]

Human Rights Council Resolution 38/5 "Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts" [109]

In 2018, the UN Human Rights Council adopted Canada-led resolution by consensus with over 50 co-sponsors from every region, establishing that online GBV is a human rights violation in need of urgent attention. The resolution indicates not just a growing recognition of the risk of violence faced by all women and girls, but also an understanding that there are those who face violence on account of gender and also multiple and intersecting forms of discrimination, and recognises that a multi-pronged approach working with all relevant parties is required. Importantly, the resolution recommends that human rights frameworks guide responses to online GBV, so that they do not further restrict women's human rights, for example, by limiting their use of encryption, or by censoring their own expression.

World Summit on the Information Society

- The UN World Summit on the Information Society (WSIS) process and its outcome documents are considered cornerstones of international norms and discourse on internet policy and governance. The two-stage WSIS took place in 2003 (the Geneva phase) and 2005 (the Tunis phase).
- The Geneva Declaration of Principles (the outcome of the first phase), which enjoyed the support of UN member states, and all relevant stakeholders affirmed the importance of ICTs for women's empowerment and that women must participate on equal footing in all spheres of decision making in the information society. Paragraph 12 of the Geneva Declaration reads "We affirm that development of ICTs provides enormous opportunities for women, who should be an integral part of, and key actors, in the Information Society. We are committed to ensuring that the Information Society enables women's empowerment and their full participation on the basis on equality in all spheres of society and in all decision-making processes. To this end, we should mainstream a gender equality perspective and use ICTs as a tool to that end." [110]
- The Tunis Agenda for the Information Society (the outcome of the second phase) reaffirms the commitment of all stakeholders to encourage women's participation in decision-making processes, by calling for "implementing effective training and education, particularly in ICT science and technology, that motivates and promotes participation and active involvement of girls and women in the decision-making process of building the Information Society.[111] Further, it recommits all stakeholders to "building ICT capacity for all and confidence in the use of ICTs by all – including youth, older persons, women, indigenous peoples, people with disabilities, and remote and rural communities – through the improvement and delivery of relevant education and training programmes and systems including lifelong and distance learning."
- In 2015 when the World Summit on the Information Society went through a 10-year review, the UN General Assembly adopted resolution 70/125 "Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society".[112] Resolution 70/125 reaffirmed the importance of promoting and maintaining gender equality and women's empowerment and guaranteeing the inclusion of women in the emerging global ICT society. Specifically, it called for "immediate measures to achieve gender equality in Internet users by 2020, especially by significantly enhancing women's and girls' education and participation in information and communications technologies, as users, content creators, employees, entrepreneurs, innovators and leaders. We reaffirm our commitment to ensure women's full participation in decision-making processes related to information and communications technologies."

[108] "Sustainable Development Goal 5: Targets and Indicators", https://sustainabledevelopment.un.org/SDG5

[109] Human Rights Council Resolution 38/5, *Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts,* https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/38/5

[110] See https://www.itu.int/net/wsis/docs/geneva/official/dop.html

[111] See https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.html

[112] UN General Assembly, *Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society,* A/RES/70/125, 1 February 2016, https://undocs.org/en/A/RES/70/125

ITU Resolution 70 (2018)

At its 2018 Plenipotentiary meeting, the member states of the ITU adopted Resolution 70, “Mainstreaming a gender perspective in ITU and promotion of gender equality and the empowerment of women through telecommunications/information and communication technologies” The resolution recognized that:

- equal access to ICTs for women and men and equal participation of both women and men at all levels and in all fields, especially in policy-and decision-making, are beneficial to society as a whole, particularly in the context of the information and knowledge society;
- bridging the gender digital divide requires fostering digital skills, education and mentorship for women and girls, so as to advance their participation and leadership in the creation, development and deployment of telecommunications/ICTs;
- there is a need to continue fostering the participation of women and girls in the telecommunication/ICT domain at an early age and to provide input for further policy developments in the required areas, so as to ensure that the information and knowledge society contributes to their empowerment;

The resolution included a number of commitments of steps to mainstream a gender perspective and advance gender equality within the ITU itself and committed member states to a number of actions, including:

- to review and revise, as appropriate, their respective policies and practices to ensure that recruitment, employment, training and advancement of women and men in the ICT sector are undertaken on a fair and equitable basis;
- to facilitate the capacity building and employment of women and men equally in the telecommunication/ICT field, including at senior levels of responsibility in telecommunication/ICT administrations, government and regulatory bodies and intergovernmental organizations and in the private sector;
- to review their policies and strategies related to the information society so as to ensure the inclusion of a gender perspective in all activities and the fostering of gender balance to secure equal opportunities through the use and appropriation of telecommunications/ICTs;
- to strengthen educational policies and study plans in science and technology and to promote and increase the interest of, and opportunities for, women and girls in STEM and telecommunication/ICT careers, including women and girls in rural and remote areas, during elementary, secondary and higher education and lifelong education;
- to attract more women and girls to study for and to pursue STEM careers, and acknowledge the achievements of leading women in these fields, particularly in innovation;
- to encourage gender-balanced representation in delegations to ITU conferences, assemblies and other meetings, as well as in candidatures for leadership roles;

Feminist Principles of the Internet[113]

The Feminist Principles of the Internet are a series of statements that offer a gender and sexual rights lens on critical internet-related rights. They were drafted in April 2014 at a meeting in Malaysia, which brought together 50 activists and advocates working in sexual rights, women’s rights, violence against women, and internet rights. After a series of local and global follow-up workshops and events a revised set of Principles was released in August 2016. Currently there are 17 Principles in total, organized in five clusters: Access, Movements, Economy, Expression, and Embodiment. Within these clusters, relevant issues like privacy, surveillance, anonymity, and violence are covered. Together, they aim to provide a framework for women's movements to articulate and explore issues related to technology.

[113] The Principles are available at https://feministinternet.org/en

Gender matters in international cyber security. It shapes and influences our online behaviour; determines access and power; and is a factor in vulnerability. As a result, malicious cyber operations can differently impact people based on their gender identity or expression.

Yet much of what is known about gender and cyber security comes from studies of online gender-based violence and gender inequality within the information and communications technology sector. Less is known about how malicious international cyber operations between states affect people differently on the basis of gender or other characteristics that may put them in positions of vulnerability.

This report helps to fill that gap. It identifies multiple gender-differentiated impacts of cyber operations with an international dimension, such as internet shutdowns, data breaches, and disinformation campaigns, and builds the case that these differentiated impacts need to be better accounted for and understood by policy-making and technical communities. The report explores the digital gender gap that exists within cyber diplomacy and policy professions. In order to improve gender diversity and women's meaningful participation, the report advocates for solutions that also address problematic underlying gender norms and stereotypes.

APC
ASSOCIATION FOR
PROGRESSIVE
COMMUNICATIONS

Association for Progressive Communications

PO Box 29755, Melville 2109
South Africa

T +27 11 726 1692
E info@apc.org

WOMEN'S INTERNATIONAL LEAGUE FOR
PEACE & FREEDOM

Women's International League for Peace and Freedom

Rue de Varembé 1, Case Postale 28
1211 Geneva 20, Switzerland

T +41 (0)22 919 70 80
E info@wilpf.org