Why gender matters in international cyber security

Authors: Deborah Brown and Allison Pytlak

EXECUTIVE SUMMARY

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. 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, the gender dimensions of international cybersecurity remain nearly unexplored. This report aims to fill that gap.[1] It relies on 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, and explores gender diversity and women's participation within cyber policy and diplomacy.

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.[2] There is, however, little data on how this

1 The report focuses 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.

2 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.

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 by examining three types of cyber incidents that may be used as a tactic in conflict in cyberspace: internet shutdowns, data breaches, and disinformation.

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; second, threats women face in cyberspace cannot easily or neatly be separated from their offline lived realities; and third, 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.

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.[3] 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 an international cyber conflict or operation. Based on interviews with people from Cameroon, Democratic Republic of Congo (DRC), Ethiopia, India (2), Iran (2), Pakistan, and Venezuela, and desk research, five themes emerged concerning the ways in which gender impacted women's experiences of internet shutdowns: personal safety, professional/economic impact, emotional wellbeing, education, and finding alternative connectivity.

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. 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. The research explored two data breaches, in Brazil and Chile, which took place in medical settings, which dramatically affected not only women's privacy but also their sexual and reproductive health rights and dignity because of the sensitivity of data breached (record on abortion and HIV status). 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.

3 See for example, 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; and Dominic Casciani, "Briton who knocked Liberia offline with cyber attack jailed", *BBC News*, 11 January 2019, https://www.bbc.co.uk/news/uk-46840461.

Disinformation

Disinformation campaigns involve the deliberate sharing and spreading of false information in order to achieve a desired goal or influence a situation. Research shows that there is a strong gender dimension in politically motivated disinformation activities.[4] As gender identity and sexual orientation are identifiers, they can become the basis on which someone is targeted to receive information across platforms. Gender norms also play a large role in direct attacks of false information. For example, women are already significantly under-represented in global media coverage of political issues[5] 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.[6] Disinformation activities perpetuate these trends and often in more malicious ways.

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. The research explored the gender dimension of disinformation campaigns, including those with links to foreign influence operations.

Participation

The rationale for improved women's participation, and gender diversity more broadly, is rooted in a simple premise: cybersecurity 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. Unfortunately, there are differences in the extent and nature of participation within all aspects of the cybersecurity field. This has been well-established within relevant technological and business sectors but also exists within cyber diplomacy and policy.

Official meeting and participation records from relevant UN meetings or events reveals strong and consistent gender imbalance.[7] 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, for example, 32 percent of 414 participants were women and 68 percent were men; while only 24 percent of delegations were led by women. [8]

When considering participation, it's important to look beyond numbers alone and ask other questions: 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

4 This report focuses 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.

5 See Global Media Monitoring Project, 2015.

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

7 Factsheet - Gender in Cyber Diplomacy, UN Institute for Disarmament Research (UNIDIR), https://www.unidir.org/publication/fact-sheet-gender-cyber-diplomacy.

8 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.

valued? Interviews conducted by the authors of the report with women working in the area of cyber diplomacy and policy illustrated other contours of gender inequality in this field. Most 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. Some highlighted that negative gender dynamics can become something that cause women to leave the profession. The reasons underpinning the gender gap in these aspects of cybersecurity are multiple, and often, context specific. In many instances the gap goes back to unequal access and/or a lack of encouragement to engage in the cybersecurity field, in any capacity. This is rooted in the prevailing patriarchal and masculine structures on which many societies are based in which women do not associate themselves with work in a "security" profession.

The key to improving participation in cyber diplomacy and policy in ways that drive change and influence policy outcomes towards greater peace and stability requires addressing the underlying gender norms that act as barriers and disincentives, as well as investing in knowledge-sharing and network-building. Approaches that go beyond "adding women" in a tokenistic way are needed, as is dedicated resourcing.

Recommendations

As a result of research conducted, the authors 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 cybersecurity strategies;
- States should utilize WPS National Action Plans or opportunities provided by other frameworks to advance women's participation within international cybersecurity, 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 cybersecurity 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 cybersecurity related work (diplomacy, capacity building, incident response, etc.);
- All actors should build intentionally supportive and inclusive spaces and work cultures in the cybersecurity 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 cybersecurity, 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: Terms and definitions

As gender perspectives are being more readily accounted for and discussed in multilateral peace and security forums it's important to have clarity and common understanding of key terminology and concepts, in order to avoid their conflation or misuse.

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.[9] Significantly, gender constructs determine who holds power, whether in families, societies, and even in global affairs.[10]

9 World Health Organization, "Gender", website, https://www.who.int/health-topics/gender.
10 UN Women, "Concepts and Definitions" website, https://www.un.org/womenwatch/osagi/conceptsandefinitions.htm.

As such, a **gender analysis**, sometimes described as 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.

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.[11] **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.[12]

Finally, there are also important distinctions to be made between **gender diversity**, **equality, equity, parity**, **and women's participation**. 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.

11 Ray Acheson, *Gender-Based Violence and the Arms Trade Treaty*, 2019, New York: Reaching Critical Will of WILPF.

12 *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.