Making Gender Visible in Digital ICTs and International Security
Report submitted to Global Affairs Canada
Prepared by Dr. Sarah Shoker

1. Introduction: Using Gender to Understand the International Digital ICT Landscape

Digital Information Communication Technologies (digital ICTs) are often understood to be a bridge towards women's social, political, and economic empowerment. Initially greeted with a wave of enthusiasm, the digital democracy of the 2000s and 2010s promised to enable active citizen-led policymaking and a bright future of e-governance (Van Dijk 2013, 2.) These promises remain, though the optimism surrounding digital democracy has increasingly given way to anxiety. Digital ICTs now redistribute global influence, sometimes to malicious actors that undermine liberal democratic norms and threaten women's rights around the world. Both weak and strong global actors have repurposed tools commonly used in cybercrime to exert international power. Coordinated misinformation on digital platforms undermine citizen trust in democratic processes (Dimock 2019). Once thought to be the solution to offline communities struggling to thrive, online communities have also became spaces for radicalization, with transnational insurgent groups and domestic white supremacist terror groups harnessing digital ICTs to reach those who were previously unreachable (von Behr et al. 2013). Machine learning software can now be used to undermine citizen privacy rights and access to equal opportunity, with racialized communities and women at increased risk of bearing the costs associated with algorithmic discrimination. Algorithmic decision-making, designed with the intention to reduce task burden for workers, threatens to re-establish what one legal scholar calls an "algorithmic Jim Crow" (Hu 2017).

This report begins to reconcile the gap between Canada's National Cyber Security Strategy (NCSS) and commitment to the Women, Peace, and Security agenda[1], with the goal being to make gender visible in ongoing discussions at the United Nations Open-Ended Working Group (UN OEWG) on digital ICTs in the Context of International Security. This report, commissioned by Global Affairs Canada, signals that Canadian policymakers are taking steps to reconcile the gap between international cybersecurity and the country's Feminist International Assistance Policy. [2] While most states with domestic ICT strategies mention women, often in relation to training opportunities and increasing women's representation in the ICT workforce, gender is largely absent from research on international security and ICTs. A 2013 study finds that the content of fourteen OECD cybersecurity strategies to be "curiously similar," with high emphasis

[1] For more information on the Women, Peace and Security agenda, its relationship to Security Council Resolution 1325, and Canada's role in the world, please visit the Government of Canada at: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/gender_equality-egalite_des_genres/women_peace_security-femmes_paix_securite.aspx?lang=eng

[2] Canada's Femininst International Assistance Policy and commitment to the WPS agenda have translated into a policy agenda that prioritizes 6 main actions areas: 1. gender equality and the empowerment of women and girls, 2. human dignity, 3. growth that works for everyone, 4. environment and climate action, 5. inclusive governance, and 6. peace and security. For more information on Canada's feminist international assistance policy, please visit: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/priorities-priorites/policy-politique.aspx?lang=eng

on critical infrastructure and technical resilience but largely silent on gender and the social impact of ICT vulnerabilities (Dupont 2013, 6). A 2016 assessment of 20 national cyber security strategies found that all studied countries focused on securing cyberspace against malicious actors, with most countries, "especially Canada, USA, UK, Germany, Netherlands," perceiving the threat to "revolve around organized cybercrimes, state-sponsored attacks, cyber terrorism, unauthorized access to and interception of digital information, electronic forgery, vandalism and extortion" (Shafqat and Massood 2016,132). In contrast, Canada, Australia, and New Zealand are among a small group of countries that mention gender mainstreaming in ICT-international security activities, though even Canada's NCSS does not mention gender or women. Rather, gender mainstreaming activities are integrated on an ad hoc basis.[3]

The aforementioned security risks have not reduced the role of digital ICTs in contemporary life. Moreover, ICTs are increasingly used to mediate the relationship between citizens and their governments. Canada's NCSS correctly identifies cybersecurity's importance to digital innovation, commercial supply chains, critical infrastructure, and the security of personal information. "We rely on digital technologies for more than personal enjoyment—they are integral to the systems that underpin our economy and our way of life" (Public Safety Canada 2018). However, when women do not have the necessary tools to participate in contemporary political life, their absence in government institutions, markets, and civil society translates into a democratic deficit. Without proper attention, gender identity risks being the difference between full membership in a community of political rights and second-class citizenship.

Within the context of international ICT diplomacy, women[4] comprised approximately 20.2 percent of total participants in the six Groups of Governmental Experts (GGEs) between 2004 and 2019. The United Nations Institute for Disarmament Research (UNIDIR) attributes growing improvements in gender representation between 2004 and 2019 to the UN Secretary-General's Agenda for Disarmament, which includes a commitment to gender parity in disarmament expert groups. By 2021, UNIDIR predicts that 40 percent of GGE delegates will be women, in contrast to 2004 when approximately 10 percent of GGE delegates were women (UNIDIR 2019.) Improved gender representation between 2004 and 2019 was not an accidental outcome. Rather, member-states have intentionally committed to improving gender representation in diplomatic meetings on digital ICTs and international security. Like their colleagues in the diplomatic sector, women are a minority of cybersecurity technical experts. According to the research firm Cybersecurity Ventures, women comprise 20 percent of the global cybersecurity workforce, with (ISC)^2 reporting a slightly better rate of 24 percent representation in the workforce (Zaharia 2020).

Several UN resolutions and declarations reaffirm "women's right to participate fully in all facets

[3] For example, the Australian Government's Department of Foreign Affairs and Trade issued a call for proposals that would award grants for projects that "improve cyber affairs," including those projects involved in the "mainstreaming [of] gender equality within cyber affairs." The grant page is now expired for this project (calls for proposals were due on February 14th), but the call for proposals were sent to academic institutions, including institutions in Canada.

[4] Most statistics on women do not disaggregate data between cisgender women and transgender women. Unless otherwise noted, this report assumes that references to women include transgender women and girls and cisgender women and girls.

of public life" (Ballington, Bardall, and Borovsky 2017, 12), an increasingly challenging goal in an ICT ecosystem where users have access to an expanding range of techniques to perpetuate violence and harassment. Gender parity is more than an exercise in numbers and having enough women in the right rooms; women's underrepresentation in diplomatic and technical fields represents both a narrowing of vital expertise and a threat to Canada's international commitments.

In general, feminist approaches to analysing security are dedicated to making women "empirically visible" in a field that has historically ignored their role in shaping international affairs (Peterson 2004, 5). Appropriately, and in addition to NGO and academic research, this report integrates field interviews from individuals in low and middle-income countries working in ICT governance. (With their consent, all individuals who were interviewed for this report are cited anonymously.) As the discussions at the UN OEWG indicate, civil society actors are increasingly calling for governments to assess the social impact of emerging technologies on marginalized constituencies. This approach not only takes seriously Canada's commitment to the Sustainable Development Goals and the Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW)[5], but a cyber security approach that makes women visible also improves the country's responsiveness to political violence. As feminist International Relations (IR) scholars have noted, the international security field has an uneven track record of predicting important international events because of its tendency to exaggerate "the simplicty of the entire political system" by focusing exclusively on state behaviour (Enloe 2004, 23). Christine Sylvester elaborates on this theme and notes that

> "[m]uch of IR actually seems unprepared for the presence, let alone the power of ordinary people in international relations, whether those people walk through the Berlin Wall and help shift the Cold War polarity, or toss out autocrats in the Arab Spring Revolutions. Ordinary people are overwhelmingly absent in [international relations] because they are not seen as key stakeholders" (Sylvester 2012, 485).

As I have written elsewhere, taking gender seriously can be a corrective for a field that routinely fails to predict shifts in the global order because of its focus on large-scale actors (Shoker 2018, 11). Though this report focuses mostly on women, Canadian policymakers are clear that a gender-aware policy analysis extends to other constituent groups, including men, members from the LGBTQIA group, persons with disabilities, Indigenous groups, and racial minorities. As feminist scholars have made clear, the words 'gender' and 'women' are not synonymous. This report also briefly explains the link between gender and radicalization of men and boys in online communities. Geographic location will also affect the way women and girls experience the social impact of digital ICTs, with differences existing between urban and rural populations and between low, middle, and high-come countries.

[5] Unless otherwise noted, this report uses the definition established by CEDAW when referencing discrimination, violence, and harassment against women. For more information on definitions and CEDAW articles, please see: https://www.un.org/womenwatch/daw/cedaw/text/econvention.htm#article1

2. Gender and ICT-Enabled Harassment and Violence

Vulnerability 1: There is a relationship between the gender digital divide and international peace and security.

Globally, there are approximately 250 million fewer women than men with Internet access (UN Deputy Secretary-General 2018**)**. In contrast to high-income countries, where women's Internet usage often exceeds men's usage, women in low-income[6] countries are a minority of Internet users, with women comprising 22.6 percent of users in Africa, 41.3 percent in Asia, and 44.2 percent in Arab states (Clement 2020). In rural areas, women are 26 percent less likely than men to use mobile internet (Sorgner et al. 2018). There are notable exceptions: highly-educated women in the developing world have similar use-rates to men, indicating that educational opportunities can increase access to and use of digital tools (Antonio and Tufley 2014, 675).

Interestingly, there is a negative relationship between digital access and gender discrimination in both the developed and developing world (*ibid, 678*). Said otherwise, higher levels of ICT engagement among women is accompanied by higher rates of gender equality, a pattern that is consistent across low, middle, and high income states. Unfortunately, many countries do not disaggregate Internet usage statistics by gender, instead opting to measure access by Internet connectivity based on household—a problem, given research that illustrates the gender digital divide persists within households (*ibid*)**.** To further complicate matters, a literature overview conducted by Clare Cummings and Tam O'Neil found that when women *do* have access to ICTs, this access does not necessarily translate to influence over social, economic, and political decision-making (Cummings and O'Neil 2015, 17). Despite these methodological caveats, there is some indication that the relationship between gender and ICTs has profound implications for international security.

Several UN member-states have highlighted critical infrastructure protection as central to their national cybersecurity strategies. In this conceptualization, digital ICTs are fundamental to sustaining contemporary state-citizen relations but also introduce technical vulnerabilities that cause policymakers to view critical infrastructure as an ecosystem "of potential future disaster and...complex landscape of response" (Colliers and Lakoff 2008, 14). Indeed, the Canadian National Strategy for Critical Infrastructure defines critical infrastructure as the "physical and information technology that facilities networks, services, and assets, which if disrupted or destroyed would have a serious impact on the health, safety, security or economic well-being of Canadians or the effective functioning of governments in Canada" (Public Safety 2009). Yet critical infrastructure protection generally means identifying technical and computational vulnerabilities in the ICT ecosystem, a remnant from traditional security policy that conceptualized insecurity as a threat to state sovereignty. Yet if critical infrastructure protection is necessary for Canadians' social well-being, then ICT failures will also have negative social consequences. At the UN OEWG, several civil society members called on member states to

[6] This report uses classifiers like 'low, middle, and high-income countries' based on criteria identified by the World Bank. For more information, please visit: https://datahelpdesk.worldbank.org/knowledgebase/articles/378834-how-does-the-world-bank-classify-countries.

conceptualize critical infrastructure protection using a human-centered lens, though 'human-centered' is still a term that needs to be explored at these meetings. Nevertheless, the message was clear: instead of viewing critical infrastructure as a purely technical system, discussions on ICTs and critical infrastructure need to make ordinary people visible.

The research on gender and ICTs has generally focused on addressing what is commonly called 'the digital divide,' defined roughly as those who have access to the "digital resources to engage, mobilise and participate in public life" and those who do not (Antonia and Tuffley 2014, 674). In comparison to men, women are more likely to be primary caregivers, responsible for energy delivery to the household, less mobile, and more prone to social isolation (Davies et al. 2020). And despite growing access to the Internet via mobile technologies, women in low and middle-income countries are still 10 percent less likely to own a mobile phone, 26 percent less likely to access the Internet through a mobile phone, and 33 percent less likely to use mobile money (CGIAR 2018). ICTs come with a list of promises designed to mitigate these challenges: ICTs facilitate political mobilization, freedom of expression, remittances between diaspora communities, increase productivity and earnings between men and women, and release women's time from care and housework so that they can participate in markets (World Bank 2012, 26)**.** For these reasons, ICT infrastructure development has been central to the women's equality agenda even as governments try to reconcile the tension between ICTs as tools that both enable political expression and perpetuate gendered harassment and violence.

According to the Tallinn Manual 2.0, a publication that compiles legal opinion on cyber conflicts that fall below the threshold of war, ICTs and Internet access are not international human rights in themselves and should instead be conceptualized as rights-enabling tools[7] (Schmitt 2018, 195). Scholars have highlighted the increasingly blurred lines between security and development activities, a relationship sometimes called the security-development nexus (Walter 2016; Duffield 2009). This is especially true when examining the relationship between ICTs, gender, and international security. State censorship and ICT filtering is negatively correlated with ICT infrastructure expansion (Shirazi et al. 2010, 27), meaning that states who restrict access to digital platforms are also the same states who are vulnerable to cybersecurity attacks on their critical infrastructure. While softening the boundaries between development and security can come with a number of moral challenges (some scholars have noted that this risks injecting defence priorities into aid initiatives, a serious problem for an international landscape still grappling with the consequences of colonization), cybersecurity remains siloed away from these discussions and relatively immune from gender mainstreaming activities, perhaps because women have been structurally excluded from designing, accessing, and using ICTs.

A gendered approach to security disrupts the domestic-international security dichotomy that is prevalent in international affairs. Since the 1980s, the scholarship on gender in International Relations has seen a proliferation of work that addresses the connection between women's equality and international conflict, to the point that some countries have entrenched policy legacies that integrate these findings into government mandates. The relationship between

[7] This report does not necessarily endorse the view that Internet access is not a human right. Rather, this view appears to be the current consensus between legal experts who study international cybersecurity law and, as such, is a view that imposes constraints upon viable policy options that would be deemed appropriate by member-states.

political violence and gender inequality within and between states is largely accepted by international organizations and several states. At the 1995 Fourth World Conference on Women in Beijing, participating governments concluded that gender equality was foundational for international peace and stability (UN Women 1995). The Government of Canada's WPS agenda similarly highlights women's involvement in government and security activities as foundational for economic growth, peace, stability, and safety (Government of Canada 2017)**.** The 2010 U.S National Security Strategy notes that "countries are more peaceful and prosperous when women are accorded full and equal rights and opportunities," and the U.S Quadrennial Diplomacy and Development Review recognizes that "the status of the world's women is not simply an issue of morality—it is a matter of national security" (2010, 23).

Feminist scholarship has demonstrated that a relationship exists between gender inequality and militarism, where some forms of political violence are understood to be a function of norms that grant individuals higher social status when traits associated with toxic masculinity, like the social and violent control of women, are performed (Caprioli 2003; Whitworth 2004)**.** As Laura Sjoberg concisely states:

> [t]he study of gender in political life is not the study of *what men do and what women do* and how they might be similar or different. Instead, it is the study of how social structures select for and value characteristics associated with masculinity and femininity, and how those selections and values influence lives of not only 'men' and 'women', but of society more generally (Sjoberg 2011, 10).

Work by Valerie M. Hudson et al. (2009) finds that indicators like the physical security of women, son preference, education gaps, exclusion of women from government, legal restrictions on women's movement in public spaces, and dress codes are superior predictors of state aggression at the international level. (Though, it is important to contextualize these conclusions; as Laura Sjoberg (2016, 534) notes, these indicators measured violent conflict in 2006, so it is unclear if these indicators hold across lengthier time periods.) Nevertheless, these authors argue that gender inequality is a better predictor of international state aggression than variables like democracy and wealth (Hudson et al. 2009, 41) .

Women's access to ICTs appears to mirror other indicators that are used to measure gender equality. (For example, when women have access to educational opportunities then they are also more likely to have access to ICTs.) There does appear to be a relationship between social unrest and ICT blockages during elections and government transitions, and it is during this period that women are more likely to be targeted with sexual violence and other forms of politicial disenfranchisement (Ballington, Bardall, and Borovsky 2017). For example, women face greater restrictions on mobility during ICT blockages, a relationship that is further explored in the case study on Internet shutdowns. If the research that establishes the relationship between women's (in)equality and violent conflict holds, then we can hypothesize that there should be a negative relationship between women's access to ICTs and intrastate/interstate violence.

When asked about the practical impact Resolution 1325 had on women in conflict zones, one worker at UNIFEM succinctly stated that "[i]t means very little to women in conflict zones unless they know about it and have the security, resources, and political space to organize and access decision-makers" (Cohn, Kinsella, and Gibbings 2004). Many of the activities that are

indicators of women's equality (like voting, driver's licenses, and property ownership) are increasingly accessed through digital platforms. If ICTs are rights-enabling tools, then their abrupt withdrawal, as in the case of Internet shutdowns, not only challenges international stability but installs numerous obstacles for women's political participation.

Vulnerability 2: Women, gender and sexual minorities experience gendered patterns of ICT-enabled political violence.

Instead of using the term 'cyberviolence,' some social scientists and policymakers prefer to use 'technology-facilitated' violence to reflect that the ICTs used to perpetrate harassment and violence are embedded in daily life and do not remain online (Power, Scott, and Henry 2018). In comparison to men, women are at increased risk of ICT-enabled harassment and violence, with transgender, lesbian, bisexual, and racialized women at even greater risk than white women (Citron and Franks 2014, 354). For minority women, including women off colour, lesbian, and transgender women, their identities become additional targets for ICT-harrasment and violence. Low, middle, and high-income countries also exhibit different patterns of gendered ICT-enabled violence, which is explored further below. Across geographic locations and identity backgrounds, perpetrators of ICT-enabled harassment and violence share a common "patterned resistance to women's public voice" (Sobieragj 2017, 2).

Though women in low-income countries are less digitally connected than their male counterparts, they are nevertheless targeted by gendered forms of political violence and harassment when they do use ICTs. Like most cyberconflict, the gendered violence that is mediated through ICTs usually falls below the legal threshold of war. Nevertheless, just as ICTs can be conceptualized as rights-enabling tools, they can also be conceptualized as tools that disrupt political life. Gabrielle Bardall (2013) finds that women are more likely to be victims of election violence and that ICTs act as a platform for spreading an already-entrenched problem. (Election violence is defined here as "any harm, or threat of harm, to any persons or property involved in the election process itself, during the election period" (Kammerud 2011, quoted in Bardall 2013, 59). Internet shutdowns are often accompanied by gendered violence against women and men, where violent political groups harness the blackout and activists lose the ability to broadcast human rights violations to a transnational audience. Or as one interview respondent who participated in the 2019 Sudanese sit-in stated: "they rape the women and kill the men" (Interview 3, 2019).

There are numerous examples of ICT-enabled techniques that are used against women during elections and government transitions. The 2008 Kenyan election was followed by post-election violence, where "tribal-based political partisans" used SMS messages to threaten opposition women with death, physical and sexual assault **(**Bardall 2013). The last five years have seen increased scholarly focus on ICT-enabled harassment and violence directed at politically active women, especially women who choose to run for political office (See: Faith and Fraser 2018; Atalanta 2018.) However, like many other policy areas, there is a dearth of systematic data collection on ICT-enabled harassment and violence against women, both during and outside government transitions. When data is collected, few states disaggregate statistical data based on gender (Cicerchia 2017, 33). Though some NGO workers have argued that the 2019 Internet

shutdown in Sudan is linked to higher rates of human rights violations (Taye 2019), the research literature still needs to explore whether this relationship holds across different countries that have experienced Internet shutdowns.

Women in high-income countries are not immune from gendered ICT-enabled violence that blurs the boundaries between digital and physical space. For example, the Kapersky Security Network found that the presence of or attempt to install stalkerware[8] had increased by 373 percent in comparison to the same period during 2018. Users in high and middle income countries are more likely to encounter stalkerware on their mobile devices, with users in the Russian Federation comprising 25.6 percent of those affected, followed by India at 10.6 percent, Brazil at 10.4 percent, and the United States at 7.1 percent[9] (Coalition Against Stalkerware 2019, 8). The study, authored by the Coalition Against Stalkerware,[10] does not identify the percentage of stalkerware victims by gender but the publication does note the link between stalkerware and intimate partner abuse, a trend that has also been identified by NGOs who work in the same field. One UK domestic-violence charity found that technology was used in 95 percent of its intimate-partner violence cases (Jee 2019), a connection that has also been made by the Electronic Frontier Foundation (Greenberg 2019) and which has similarly inspired an entire series of investigative journalism at the U.S-based *Motherboard* (2019). Additionally, smart home devices (thermostats, Google nests etc.) are becoming increasingly common means of control in intimate partner violence, causing some social scientists to again note the porous borders between online and offline violence and harassment (Valentino-Devries 2018).

Academic research on this topic is still nascent, but one U.S study finds that most spyware masquerades as dual-use software, often marketed for child-safety or as an anti-theft consumer tool (Chatterjee et al. 2018). From the Canadian academic landscape, the Citizen Lab at the University of Toronto has found that legal remedies available under Canadian consumer privacy law were too limited to "establish deterrence or ex post remedy and enforcement" (Parsons et al. 2019). Even when stalkerware is legally understood to be a form of cybercrime instead of international cybersecurity, Canada's WPS agenda would suggest that women's rights 'at home,' including safety from intimate partner violence, is not merely a domestic issue. Though intimate partner violence impacts all genders, police-reported data in Canada states that women comprise 82 percent of victims in heterosexual relationships. For same-sex couples, 55 percent of victims are men (Ibrahim 2017). However, police-reported data has its limitations; Statistics Canada estimates that more than 80 percent of IPV cases go unreported (Kingston 2019).

Gender-based attacks that use digital ICTs are designed to silence women's voices and presence in online and offline spaces. "Women's use of public space is shaped by the looming possibility

[8] The Coalition Against Stalkerware defines stalkerware as "software, made available directly to individuals, that enables a remote user to monitor the activities on another user's device without that user's consent and without explicit, persistent notification to that user in order to intentionally or unintentionally facilitate intimate partner surveillance, harassment, abuse, stalking, and/or violence." For more information, see: https://stopstalkerware.org/about/what-is-stalkerware/.

[9] It should be noted that the Kapersky Security Network is a Russian company and the study analysed mobile devices that used Kapersky software, meaning that Russian users could be overrepresented in the sample.

[10] The Kaspersky Security Network is a Coalition Against Stalkerware member.

of gender-based incidents that threaten to undermine their freedom, comfort, and safety" (Sobieraj 2017, 1). These attacks can include doxxing, a technique of intimidation that publicizes where a woman lives or works and which subsequently places her at greater risk of offline harassment and violence (*ibid*, 6). Doxxing would not be an effective technique of intimidation if women did not experience gender-based violence offline, but online harassers use ICTs to remind women of their precarious social standing in a political community where they must take extra care to protect themselves from gendered forms of insecurity. In 2015 for example, Planned Parenthood, the largest reproductive health care provider in the United States, suffered both DDoS (distributed denial of service) attacks and a doxxing of their employee database from anti-abortion hackers (IGF 2015, 18). The hackers successfully breached Planned Parenthood's database—inadvertently presenting another argument for encryption without backdoors. The attack was intended to be both punitive, by punishing healthcare workers who provided reproductive healthcare, and destructive, by hindering women's access to healthcare and physical security.

Doxxing is one of many ICT-enabled forms of harassment and violence. Other common harrasment techniques include unauthorized pornography, like so-called revenge porn, the use of hidden cameras, and spreading photos of women who are intoxicated without their consent. Women are also commonly targeted with verbal attacks that centre their bodies and femininity to discredit their expertise and online presence (Sobieraj 2017). There is also some indication that gender and sexual minorities experience greater levels of digital harassment, with transgender individuals experiencing higher volumes and different forms of harassment in comparison to cisgender individuals. Called 'polyvictimization' by the study's authors, transgender women and men were most likely to experience 25 out of 26 identified forms of digital harassment (Powell, Scott, Henry 2018, 20).

Some scholars argue that violence against women is linked directly to a state's incapacity to respond to violence within its own borders (Htun and Jensenius 2020, 145). Rather than being viewed as a distinctive form of violence, this argument positions violence against women as an extension of the same violence directed at politically active men; both groups suffer the consequences of living in states with weak democratic institutions (Piscopo 2016, 437). Other researchers have responded to these criticisms by pointing to the experiences of female activists and politicians in states with strong democratic institutions and with the capacity to enforce criminal law (Krook and Sanin 2016, 465,). Examples include graphic photos and threats directed at the Italian speaker of parliament, rape threats over Twitter directed at UK parliamentarians, and complaints that a "toxic culture" of sexual harassment existed across all political parties in Australia's parliament (*ibid*, 478).

Consequently, strong state capacity likely matters, but even strong institutions contain gendered relationships that are not always self-evident at first glance**.** As highlighted by the EU Agency for Fundamental Rights (EUFRA), higher numbers of sexual violence reported to the police may actually be a response to a system that encourages reporting rather than being an accurate depiction of sexual assault trends across member-states. For instance, EU member states like Sweden report 47 sexual assault cases per 100, 000 people, while Greece and Hungary report 2 cases per 100, 000 people. These reporting numbers do not mean that there are fewer sexual

assault incidents in Greece and Hungary but that "higher recorded figures" indicate "that the system for...recording and prosecution of rape is working" (EUFRA 2015, 14). State capacity might also influence the tools that are used to target women. "[I]n countries where violence is routine, it may be 'easier' to use physical, sexual...violence," whereas "high levels of state capacity, ironically, [can provide] stronger guarantees regarding the right to free speech, which might be mobilized to defend this behavior" (Creasy 2014, quoted in Krook and Sanin 2016).

Vulnerability 3: Online communities can act as spaces for the radicalization and recruitment of men and boys.

Almost all research on modern terrorism finds a relationship between digital media platforms and radicalization, though it is not always clear whether the growing number of online extremist websites cause, rather than correlate, with radicalization (von Behr et al. 2013, 17). In general, the literature on extremist violence sees the Internet as an "accelerant" to radicalization, where extremist ideas are normalized within a community of individuals who validate each other. As masculinities scholar Michael Kimmel notes, the majority of individuals who perpetuate non-state political violence are men, a commonality that stretches across the ideological spectrum (Kimmel 2018). They are also more likely to be targeted and recruited into politically violent groups (Shoker 2018, 42). The last five years have seen a proliferation of articles with titles like "We need to talk about the online radicalisation of young, white men" (Wilkinson 2016), "Swallowing the Red Pill: a journey to the heart of modern misogyny" (Marche 2016), and "Racists are recruiting. Watch your white sons (Schroeder 2019). These articles point to online subcultures that recruit boys and men based on shared grievances related to race, class, and gender.

Online communities shrink geographic distance, with individuals who were previously physically separated suddenly able to socialize and share extremist content (von Behr et al. 2016). Some studies have highlighted digital reach as an important factor for reaching women who joined ISIS (*ibid*). In addition, algorithmic recommender systems on digital media platforms have become increasingly important for understanding how ICTs can normalize violent extremist content, though trying to summarize the emergent literature on this topic without computer-assisted content analysis would be an impressive challenge. A single search on Google Scholar for "Youtube extremist content" yields 2,710 scholarly publications from January 2019 to February 2020.

Some of these online communities have been responsible for perpetuating cyberharassment against women, with doxxing and threats of physical and sexual violence being some of the more common tactics used to target feminist activists**.** Some high-profile cases have resulted in women leaving their homes for fear of their safety (Mother Jones 2014). Increasingly, reporters have highlighted the relationship between 'lone wolf' mass shooters like Elliot Rodgers and vehicle-ramming attacker Alek Minassian and their involvement with online communities in incel subreddits and forums on 4Chan (Baele, Brace, and Coan 2019). Though mass shooters are not ideologically identical, they do appear to share a history of violence and misogyny (Bosman, Taylor, and Arango 2019). Whether violence against women is a causal variable or useful predictor for ideological gun violence within democratic countries largely remains unexamined.

(Though answering this question would be useful given the research that has found that certain forms of violence against women are predictors of international aggression and intrastate stability.) Moreover, while sociologists point to the important role gender occupies in extremist violence, another important variable persists across these attackers: nearly all mass shootings occur in liberal democratic countries, indicating that regime type may influence an attacker's type or style of violence.

Case Study 1: Internet Shutdowns

Despite the increasing number of Internet shutdowns that are occurring worldwide, there is still remarkably little data about the gendered impact of Internet shutdowns. Yet since at least the 1990s, disaster and emergency-preparedness scholars have noted that women face a different set of challenges during critical infrastructure emergencies (Fothergill 1996; Yasmin 2016; Davis et al. 2020). Internet shutdowns are politically orchestrated critical infrastructure failures and often occur during periods of civil unrest. Internet shutdowns (sometimes called Internet blackouts or blockages) are distinct from Internet content filtering, the latter which is a growing practice in states across all regime types. A relatively rare practice into the early 2000s, over 40 states now practice some form of Internet content filtering and approximately 960 million people live with some form of Internet censorship (Diebert 2012, 269). Some scholars have conceptualized Internet shutdowns as one tactic in an arsenal of tools that range from content filtering, to coordinated misinformation, to arresting individuals for online political expression (Diebert and Rohozinski 2010, 7). Several NGOs, however, have opted to mark Internet shutdowns, including partial shutdowns that impact social media platforms, as a distinctive phenomenon. While content filtering has proliferated since September 11th, 2001 amongst all regime types, Internet shutdowns are perceived to be a newer form of information control, with one organization reporting that Internet shutdowns cost the world $8 billion dollars in 2019 (Woodhams and Migliano 2020.) According to Freedom House, approximately 46% of the world's population live in countries where the Internet or mobile network was disconnected in 2019, "often for political reasons" (Shabaz and Funk 2019, 2).

In 2019, there were 122 Internet shutdowns and social media blockages, with Whatsapp being the social media platform blocked most frequently (Woodhams and Migliano 2020). These numbers were slightly better than the number of Internet shutdowns in 2018. Out of 196 verified Internet shutdowns in 2018, political leaders attributed the shutdown to fake news and hate speech 33 times, surpassed only by appeals to national security and public safety (Taye and Cheng 2019)**.** Internet shutdowns are increasing worldwide, from 106 in 2017 to 196 in 2018 and with Asia and Africa being the most affected countries (*ibid*.) Though political leaders do not justify Internet shutdowns by pointing to women's protection, they have increasingly argued that Internet shutdowns are necessary to prevent violence spurred by misinformation on social media. In less than 10 years, Internet shutdowns have become normalized and perceived as viable responses to quelling both peaceful political mobilization and violent political protest.

The literature on international governance usually paints liberal democracies as the actors responsible for setting the normative agenda within international society (Finnemore 1996; Heller and Khal 2013; Katz 2017). Traditionally, researchers have sought to explain how 'good'

norms that are associated with liberal democracy, like protecting human rights, are spread throughout the international system and adopted by non-democratic states (Risse-Kapan, Ropp & Sikkink 2013; Porter and Webb 2009). However, the literature on international governance overwhelmingly explains this socialization process as one where non-Western states adopt the normative preferences of liberal democracies (Xiaoyu 2012; Ndi 2017). Recent research has highlighted that 'bad' norms can also be diffused throughout the international system and that non-democratic states can act as important norm entrepreneurs in the international system. One Internet governance expert I interviewed argued that though his own Caribbean island was relatively liberal and embraced free market economics, some government elements were beginning to entertain social media blockages and Internet shutdowns as viable solutions to the problem of political misinformation and 'fake news.'

> Even my country, which is fairly liberal, sees that if Hong Kong can do it, if India is doing it—**w**hich are fairly well-developed countrie**s**—**t**hen why can't we do it in our own country? Why not shutdown Whatsapp, because what use is it serving other than spreading political misinformation? And my country is not a military dictatorship. But if you see another country doing it, then it becomes the norm. I'm not aware of any country that has been sanctioned over an Internet shutdown, are you? (Interview 3, 2019)

In part, some new democracies may be tempted towards Internet shutdowns because they lack the capacity to respond to misinformation. "You can sue a newspaper in a local court, but you can't sue Facebook...In the traditional world, you can revoke their license, but that can't happen with Facebook or Whatsapp" (Interview 3, 2019). Specifically, violence during election time seems to be perceived as particularly problematic by political leaders and Internet shutdowns are often accompanied by government-led violence against their own constituents. "You're going to see this problem proliferating in the next five years, every time there's an election, every time there's social unrest" (Interview 3, 2019).

Another interviewee working on women's rights in the MENA region stated that the normalization of Internet shutdowns was increasingly problematic for women rights activists because ordinary people changed the way they related to the Internet. "The people get used to censorship to the point that they start censoring themselves. The government doesn't need to intervene; people are frightened and they see the consequences of internet shutdowns [which usually involves] surveillance and people being targeted by other civilians. You don't need to be followed by a government representative since people will follow you [online], especially if you're working on women's rights" (Interview 1, 2019). This interviewee stated that women's activism had become more politically difficult in a post-Arab Spring environment.

> I have found that people are too focused on the Arab Spring...it has been 8 years since the Arab Spring...we need to talk about the implications and consequences of technology in a post-Arab Spring environment...the Yemen of today was not the Yemen of 8 years ago. The mindsets have changed, the people have changed." This interviewee noted that being a politically active woman came with greater risk now in comparison to the Arab Spring environment (*ibid*).

NGOs have noted that communication blockades are particularly problematic when trying to work with vulnerable populations. In Kashmire, which was frequently targeted in 2018, women's rights activists struggled to provide counselling to women who were targeted with domestic violence. Communication lines were blocked and NGOs could no longer provide their standard

services to population groups that now faced the double burden of domestic and government-led violence (Bakshi, 2019). These personal reports largely replicate the larger findings from research on gendered violence during national emergencies and financial crises, a time when women experience higher rates of sexual assault [11] and intimate partner violence from male partners who have experienced job loss (Davis et al. 2020). When I asked my interview participant how NGOs continue to serve their constituencies during Internet shutdowns, she responded by saying they "basically don't. We lack social services even without internet shutdowns, so imagine what happens during Internet shutdowns. When women need access to social services, then they're going to access programs using traditional mouth to mouth methods" (Interview 1, 2019).

One interviewee who participated in the 2019 Sudanese sit-in[12] said that the Internet shutdown impacted girls and women more than their male counterparts. (The June 3rd sit-in was disrupted by the Transitional Military Council and was later dubbed the 'Khartoum massacre' after more than 100 people were killed.) Women and girls "are less likely to be allowed by their parents, guardians, or even husbands to leave the house. So we depend more on the Internet to connect us to the news and to mobilize" (interview 4, 2019.) This particular activist said that online spaces held distinct advantages for women, as women's offline mobilization came with increased risks to physical safety and harassment. The participant stated that while women still experience gendered harassment online at higher rates than their male counterparts, women who do not use their real names are protected by anonymity and are less likely to experience physical violence than those who mobilize offline. The participant also mentioned that in offline workshops and political events, male participants often took 'more floor space' and that women had less opportunity to voice their own political ideas, whereas Twitter and Facebook groups presented a curated space that could be led by women.

Facebook and Twitter usage is very common in Sudan. "Each person is in at least 5 Facebook groups. I'm in 10 groups" (Interview 4, 2019). Their popularity, she explained, was due to the fact that these Facebook groups functioned as e-commerce sites; digital transactions through formal banking institutions are relatively new to Sudan**,** so Facebook groups are a viable alternative for merchants to reach their consumer base. In December 2018, after the Sudanese military removed Omar-Al Bashir from office and established the Transitional Military Council, these Facebook groups were transformed into political spaces. For example, one Facebook group run by women that was designed to expose and identify men who cheated on their intimate partners (much to the irritation of some Sudanese men) morphed into a space where they would identify and expose men associated with the Transitional Military Council, many of whom were accused of entering the sit-in while undercover and perpetuating sexual violence against women activists.

---

[11] For example, shortly after the 2014 Ebola epidemic, there was a spike in teenage pregnancies caused by sexual assault during the epidemic in Liberia, Guinea, and Sierra Leone. See: Yasmin, Seema. 2016. "The Ebola Rape Epidemic No One's Talking About." *Foreign Policy*, February 2. https://foreignpolicy.com/2016/02/02/the-ebola-rape-epidemic-west-africa-teenage-pregnancy/.

[12] For more information on the Sudanese protests, Omar al-Bashir's resignation, and the transitional military council, see Human Rights Watch 2019: https://www.hrw.org/world-report/2020/country-chapters/sudan.

The Internet shutdown created further restrictions on women's mobility. Women were less likely to participate as the sit-ins turned increasingly violent, increasingly using Internet access for situational awareness. "If there are guns outside your house, at least you have the Internet and there are people telling you something is happening here and there, at least you don't feel alone" (Interview 4). Online communities functioned as an informal crowdsourced violence warning system, where Twitter and Facebook users were able to broadcast location data about civil violence. In particular, Facebook Live became useful for documenting real-time political violence since users could expect that these videos were authentic and undoctored. Interview participants noted that given the normalization of Internet shutdowns, grassroots members had become quite good at predicting when governments would restrict access to ICTs.

In the case of the 2019 Internet shutdown in Sudan, activists anticipated some form of ICT blockage and users began posting online instructions about connecting to Virtual Private Networks (VPNs) in an attempt to circumvent what they thought would be another social media blockage (but that became a full Internet blackout). As a result, speech on social media can act as a good warning signal for the international community and for predicting politically-orchestrated ICT failures. For now, VPNs remain a popular option for users who want to work around Internet blockages, though government authorities have begun erecting barriers to VPN access. For instance, users in India-controlled Kashmir who use VPNs to circumvent social media blockages are now at risk of being legally prosecuted, with authorities opening a case against at least one hundred people in the Himalyan region (Singh 2020).

3. Using Digital ICTs to Prevent Gender Violence

Internet shutdowns do not necessarily cancel political mobilization—the 2011 Arab Spring protests in Egypt only grew in response to the Mubarak Government's Internet shutdown and women found ways to mobilize in the absence of ICTs. Though women in low-income countries are less likely than men to have Internet access, women in Egypt are better represented online than in traditional media (Cattle 2016, 434). While a gendered digital divide remains, access to ICTs still comprises a substantial portion of women's political participation.

> Data from 2011 indicate that 36% of Egypt's Facebook population was female, while 33% of Egyptians active on Twitter during the protests were women. While these numbers admittedly translate to a ratio of about two men for every woman using social media, they still represent a significant increase in representation when compared to statistics reflecting female representation in traditional media (*ibid*).

The Arab Spring also revealed the high rates of sexual harassment experienced by Egyptian women. A study by UN Women found that that 99% of 2,334 women sampled across 7 governates had experienced sexual harassment, a study that has been replicated by independent researchers and local not-for-profit organizations (Abdelmonem and Galan 2017, 154). Though Egypt's penal code criminalizes sexual harassment, women seldom report cases of sexual harassmemt (Sadek 2016, 1-2). In this regard, Egyptian women mirror a worldwide trend: less than 40% of women and girls worldwide who experience violence report these crimes or seek help (Kelly and Johnson 2020, 13).

In response to the gendered political violence that accompanies elections and government transitions, women's rights advocates have built a vibrant software ecosystem that encourages social change. HarassMap, an Egyptian non-profit volunteer organization founded in 2010 and best known for its interactive mapping application that goes by the same name, created a crowdsourced map using the Google Maps API. Users can report incidents of sexual harassment in real-time through Google Maps, SMS text messages, and an online public noticeboard. HarassMap acts as a "[a] complex digital artifact whose...influence and connections extend far beyond the limits of the digital sphere…[T]he map blurs the...sets of relations [that] are established continuously between the online and offline words" (Bernadri 2017, 224). The success of HarassMap has been replicated by other organizations—Akshara, a Mumbai-based not-for-profit women's organization, launched HarassMap Mumbai in 2013.

Increasingly, women's rights advocates are using digital ICTs to build resilience in the face of social disruption. These technologies are born in turbulent political climates, where regime change also highlights the precarious status of women's political and social rights. Ushahidi Inc. was borne from the violence surrounding the 2007 Kenyan presidential election, where users could send texts and link photos of violence to particular geographic locations on Google Maps. Initially an election monitoring tool, Ushahidi has since expanded to log violence in countries impacted by natural disasters, like Haiti, New Zealand, Australia, and the United States. Importantly, HarassMap also uses Ushahidi software, indicating a transnational network of resource sharing and learning between stakeholder groups. Women's rights advocates have used digital ICTs to build platforms where "ordinary people are repositories of knowledge about wars" and where "their memories are crucial log-books in constructing a war narrative" (Parashar 2013, 626). Whether ICT-enabled solutions emerge in response to long-term trends, as in the case of HarassMap, or in response to short-term bursts of electoral violence as in the case of Ushahidi, women's resistance 'at home' is linked to the international security moment.

Many of these ICT 'work arounds' are borrowed from offline spaces, where women adopt a series of adaptive measures to reduce the chance that they will become targets of violence and harassment. Women will use digital ICTs to determine which spaces are open to them, as in the case of Sudanese activists who relied on social media to assess the safety of offline spaces. However, these adaptive measures are not limited to low and middle-income countries. For instance, some teenage girls and boys in the United States have used TikTok to record fake conversations for girls and women who feel unsafe in rideshare vehicles like Uber and Lyft. (In 2018, Uber reported more than 3000 sexual assaults in U.S rides alone (Associated Press 2018).) The conversations are meant to be played aloud, thereby imitating a speaker phone, and they signal to the driver that someone is both waiting for the woman and that her GPS location is visible to her friends. These Tiktok videos are accompanied by written messages like "[h]i ladies, use this and stay safe if you get into a sketchy Uber/Lyft." [13]

These methods of resilience exist at the intersection of online and offline lived experiences. They are intelligently and imaginatively constructed. The videos harness in-group solidarity against a

[13] As is typical on social media platforms, a number of 'tweets' are authored by pseudonymous authors and become a collaborative effort between several users. For a thread of TikTok video examples, see: https://twitter.com/haaniyah_/status/1238800078577549313.

common threat of gendered violence in public space. These videos rely on decentralized social networks and are not-coordinated by formalized leadership; they are voluntarily recorded by individuals and like other trends on social media platforms, rely on the message's viral power to recruit interested individuals to record similar videos. While some pundits have argued that so-called 'hashtag activism' is an insufficient tool for political mobilization—sometimes called 'slacktivism' to illustrate the relatively low-cost of promoting hashtags on one's own social media account— hashtags have successfully been used to create borders around online communities by allowing users to identify other individuals who share a commitment to certain norms. Other scholars have argued that high profile cases like the #BringBackOurGirls and the #MeToo campaigns signal that the 'new social movements' are integral to today's 'network society' (Smith 2015, 16). They are less hierarchical, more interactive, and deliberately try to forge human rights-centred political relationships by engaging in a "discursive struggle" that contests authority (Cohen 1985, quoted in Smith 2015, 16). These movements are generally transnational and, as demonstrated by the criticism directed at the Nigerian Government's slow response[14] to rescue the girls abducted by Boko Haram, invoke international norms that 'name and shame' norm violators. The diffusion of these social norms are dependent upon the physical integrity of the network.

Not only do online communities require stable networks in order to mobilize, but women's rights advocates are increasingly reliant on privacy-enhancing technologies, such as end-to-end encryption offered through applications like Whatsapp, Signal, and Threema, to facilitate human rights activism. The importance of privacy enhancing software applications has been underscored by the UNHRC**,** whose Special Rapporteur stated that "encryption and anonymity, separately or together, create a zone of privacy to protect opinion and belief...and can shield an opinion from outside scrutiny, particularly important in hostile, social, religious and legal environments" (Kaye 2016, quoted in Deeks 2016, 3). The recent communique published by law enforcement members in the Five Eyes intelligence community, which calls for tech companies to avoid developing "end-to-end encryption in ways that empower criminals or put vulnerable people at risk," risks jeopardizing already marginalized groups who use digital ICTs to mobilize for human rights (UK Home Office 2019)**.** As I have written elsewhere, policymakers will sometimes leverage women's and marginalized minority experiences to justify international measures that can, in reality, perpetuate insecurity for the very demographics they claim to be protecting (Shoker 2018.)

Finally, I note that many of these ICT-enabled forms of resistance place the onus of protection on demographic groups that are already at the highest risk of being targeted with violence. While these remedies are designed to treat the symptoms of gender inequality by carving a space for women to continue participating in public life, they do not necessarily alter the legal frameworks that allow perpetrators to target women in the first place.

[14]The Government of Nigeria was criticized for its poor response to the Boko Haram threat and consequently "emboldening" the group to kidnap almost 300 Chibok schoolgirls . For more information, see Nnamdi Obasi, 2015: http://america.aljazeera.com/opinions/2015/1/nigerias-faltering-response-emboldens-boko-haram.html

4. Conclusion and Recommendations

On March 12th, 2020, Tim Berners-Lee published an open letter to mark the World Wide Web's 31st birthday. Berners-Lee, credited for the creation of the web, wrote that "the web is not working for women and girls" because of "online harms facing women and girls -especially those of colour, from LGBTQ+ communities and other marginalized groups" (Berners-Lee 2020). Policy recommendations have so far focused on creating programs that narrow the gender digital divide, cultivating legal remedies for marginalized groups that have experience ICT-enabled harassment and violence, protecting privacy-enhancing ICTs from policies that would degrade their effectiveness and prevent advocates from reaching their constituents, and increasing women's representation in technical and policy fields. In addition to these policy recommendations, which have been outlined by Berners-Lee's Contract for the Web, OHCHR, the Internet Governance Forum and others, this report also offers two recommendations designed to support research efforts in the ICT and international security field.

Recommendation 1: Policymakers in member-states should be encouraged to collect statistics that are disaggregated by gender. Depending on state capacity and resources, statistical data collection can be challenging and burdensome. Nevertheless, coordination and resource sharing between member-states offer potential pathways for data collection that meet the necessary standards for evidence-based policy formation. Currently, academics and NGOs are responsible for this task, resulting in a patchwork of important studies authored in different countries but that are nevertheless ill-suited for analysing macro-level global trends that capture women's experiences with digital ICTs.

Recommendation 2: As explained in section 2, scholarship on gender and international security has noted the positive relationship between state stability and women's rights. However, little research currently exists that examines the relationship between the gender digital divide and international peace and stability. States should consider investing in research that examines whether women's access to digital ICTs are a positive indicator for international peace and stability. As states attempt to mainstream gender into their foreign policy activities, this type of research exploration can highlight where resources should be allocated to support international stability that centres human rights.

Rationale: This report does not provide a systematic literature review because the field remains fragmented and burdened by poor data collection practices. Researchers still struggle to measure the digital divide. While Canada and other high-income states collect ICT-use statistics disaggregated by sex, 'gender neutral' data collection remains the norm within low and many middle-income countries. Countries that collect gender ICT statistics are also usually the countries that have close to gender parity in ICT usage (Hafkin and Huyer 2007.) In general, research that assesses the gendered digital divide has done so using qualitative and comparative methods that are at the discretion of the researcher. The research points to an environment where gender-based ICT inequality is empirically verifiable, but the unsystematic character of the available data presents a challenge to policymakers who would like to use gender-specific indicators to measure societal change over time**.** The discrepancy between ICT data collection in high-income and low-income countries also risks erasing women in the developing world from

the international ICT policy conversation. “Much like the digital divide, a statistical divide exists where the need is greatest—in developing nations” (Huyer et al. 2005, 194 quoted in Hafkin and Huyer 2007, 26). Current efforts to rectify this situation are being led by private industry leaders. The global statistics cited in section 2 of this report use the GSMA’s Gender Identification and Analysis Toolkit (GAIT), a machine learning algorithm that “analyses mobile usage patterns to estimate the gender of subscribers.” Like other machine learning algorithms, GAIT uses machine learning to predict gender usage patterns with an accuracy rating of 84.5% based on a pilot of the project in Bangladesh (CGIAR 2018). While these efforts are commendable, they also leave statistical analysis to industry associations who have priorities outside of public accountability to a nation’s citizens.

In 2013, the UN General Assembly adopted a consensus resolution that acknowledged the growing range of ICT-enabled techniques that were being used to target women (UN Resolution 2013, 68/181). In 2018, this message was reiterated by the Deputy-Secretary General who not only called for better data collection, but stated that online violence was “part of a broader continuum of violence” and a “manifestation of discrimination against half the world’s population.” Online perpetrators shared the same paradigm as those who perpetrated gendered violence offline: “to control and silence women and girls...from participating and benefitting equally from these spaces” (Mohammed 2018). In response to these threats, global constituencies have become increasingly adept at navigating the new ICT ecosystem and have responded to transnational instability by building tools that facilitate access to the full range of their political and social rights. Policymakers may be tempted to analyse the gendered impact of ICTs as a form of cybercrime, but the boundaries between cybercrime and international cybersecurity are already tenuous at best. While the end of the Cold War and the international consensus on human security have caused states to rethink ‘what counts’ as security, the absence of gender in digital ICTs and international security should be further reconciled. In particular, the link between the gender digital divide and global peace and stability provides a route for exploring whether women’s improved access to ICTs can also have positive transnational effects on the international community.

Liberal democratic values are not only sustained by shared norms across political communities but by physical and digital infrastructures that make democratic participation possible. In contemporary life, digital ICTs act as the infrastructure that enable this democratic participation. ICT-enabled harassment and violence threatens access to the full range of rights and freedoms that are supposed to be guaranteed to all members of a political community. These threats are not insurmountable, but they do require making women and marginalized groups visible in domains that have struggled to integrate these groups in the policy process.

References

Abdelmonem, Angie and Susan Galan. 2017. "Action-oriented responses to sexual harassment in Egypt: The cases of Harassmap and WenDo." *Journal of Middle East Women's Studies* 13(1): 154-167.

Antonia, Amy and David Tuffley. 2014. "The Gender Digital Divide in Developing Countries." *Future Internet* 6: 673-687.

Associated Press. 2019. "Uber reports more than 3,000 sexual assaults during U.S. rides in 2018." *Global News*, December 5. https://globalnews.ca/news/6261375/uber-sexual-assaults/.

Atalanta. 2018. "(Anti)Social Media: The benefits and pitfalls of digital for female politicians." *Atalanta*, March 1. https://www.atalanta.co/antisocial-media

Baele, Stephane, Lewys Brace, and Travic Coan. 2019. "From 'incel' to 'saint': Analysing the violent worldview behind the 2018 Toronto attack." *Terrorism and Political Violence*, 1-21.

Bakshi, Asmita. 2019. "India is the internet shutdown capital of the world." *Livemint*, December 8. https://www.livemint.com/mint-lounge/features/inside-the-internet-shutdown-capital-of-the-world-11575644823381.html

Ballington, Julie, Gabrielle Bardall and Gabriella Borovsky. 2017. *Preventing violence against women in elections: a programming guide.* New York: UNDP and UN Women.

Bardall, Gabrielle. 2013. "Gender-specific election violence: The role of Information and Communication Technologies." *Stability: International Journal of Security and Development* 2(3): 60-71.

Bernardi, Chiara Livia. "HarassMap: The Silent Revolution for Women's Rights in Egypt." In *Arab Women and the Media in Changing Landscapes*. Edited by Elena Maestri and Annemari Profanter, 215-228. Switzerland: Palgrave MacMillan.

Berners-Lee, Tim. 2020. "Why the web needs to work for women and girls." *Web Foundation*, March 12. https://webfoundation.org/2020/03/web-birthday-31/

Bosman, Julie, Kate Taylor, and Tim Arango. 2019. "A common trait among mass killers: hatred towards women." *The New York Times*, August 10. https://www.nytimes.com/2019/08/10/us/mass-shootings-misogyny-dayton.html.

Cattle, Amy. 2016. "Digital Tahrir Square: An Analysis of Human Rights and the Internet Examined through the Lens of the Egyptian Arab Spring." *Duke Journal of Comparative and International Law* 26: 417-449.

Caprioli, Mary. 2003. "Gender Equality and Civil Wars." CPR Working Papers no. 8. Social Development Department, Environmentally and Socially Sustainable Development Network, September. http://documents.worldbank.org/curated/en/989601468762305507/pdf/270910Gender0e1PR0Wp0no10801public1.pdf

CGIAR. 2018. "The GSMA's gender analysis and identification toolkit (GAIT)." *GSMA, Mobile for Development*, August 31. https://www.gsma.com/mobilefordevelopment/resources/the-gsmas-gender-analysis-and-identification-toolkit-gait/.

Chatterjee, Rahul, Periwinkle Doerfler, Hadas Orgad, Sam Havron, Jackeline Palmer, Diana

Freed, Karen Levy, Nicola Dell, Damon McCoy, Thomas Ristenpart. 2018. "The spyware used in intimate partner violence." IEEE Symposium on Security and Privacy, San Francisco, July 26.

Cicerchia, Federica. 2017. "Women and ICTs: An analysis of social cultural and economic factors relating to gender and ICTs." Thesis, Luiss Quarantesimo.

Citron, Danielle and Mary Anne Franks. 2014. "Criminalizing Revenge Porn." *Wake Forest Law Review* 49:345-392.

Clement, J. 2020. "Global internet usage rates 2019, by gender and region." *Statista*, January 28. https://www.statista.com/statistics/491387/gender-distribution-of-internet-users-region/

Cohn, Carol, Helen Kinsella and Sheri Gibbings. 2004. "Women, Peace and Security Resolution 1325." *International Feminist Journal of Politics* 6(1): 130-140.

Collier, Stephen and Andrew Lakoff. 2008. "The Vulnerability of Vital Systems: How 'Critical Infrastructure' Became a Security Problem.'" In *The Politics of Securing the Homeland: Critical Infrastructure, Risk and Securitisation.* Edited by Myriam Dunn and Kristian Sobey Kristenson. New York: Routledge.

Cummings, Clare and Tam O'Neil. 2015. *Do digital information and communications technologies increase the voice and influence of women and girls: A rapid review of the evidence.* London: ODI Research Reports and Studies. https://www.odi.org/publications/9499-do-digital-information-and-communications-technologies-increase-voice-and-influence-women-and-girls

Davis, Sara, Sophie Harman, Jacqui True, Clare Wenham. 2020. "Why gender matters in the impact and recovery from Covid-19." *The Interpreter,* March 20. https://www.lowyinstitute.org/the-interpreter/why-gender-matters-impact-and-recovery-covid-19.

Deeks, Ashley. 2016. *The International Legal Dynamics of Encryption.* Stanford, California: A Hoover Institution Essay, Series Paper No. 1609. https://www.hoover.org/sites/default/files/research/docs/deeks_webreadypdf.pdf.

Department of State and the United States Agency of International Development. 2010. *Leading Through Civilian Power: The First Quadrennial Diplomacy and Development Review*. Middletown, January 12.

Dimock, Michael. 2019. "An update on our research into trust, fact and democracy." *Pew Research Center,* June 5. https://www.pewresearch.org/2019/06/05/an-update-on-our-research-into-trust-facts-and-democracy/

Diebert, Ronald and Rafal Rohozinski. 2010. "Beyond Denial: Introducing Next-Generation Information Access Controls." In *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace.* Edited by Ronald Diebert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. Cambridge: MIT Press, *3-15.*

Diebert, Ronald. 2012. "The Growing Dark Side of Cyberspace (...and what to do about it)." *Penn State Journal of Law and International Affairs*, 1(2): 260-274.

Duffield, Mark. 2010."The Liberal Way of Development and the Development-Security Impasse: Exploring the Global-Life Divide." *Security Dialogue* 41(1):51-76.

Dupont, Benoit. 2013. "The proliferation of cyber security strategies and their implications for

privacy." In *Circulation internationale de l'information et sécurité."* Edited by Karim Benyekhlef and Esther Mitjans, 67-80. Montreal: Les Editions Themis.
Enloe, Cynthia. 2004. *The Curious Feminist: Searching for women in the new age of empire.* Berkeley: University of California Press.
European Union Agency for Fundamental Rights. 2015. "Violence against women: an EU-wide survey." *European Union Agency for Fundamental Rights.* Vienna, Austria.
Faith, Becky and Erika Fraser. 2018. "Digital Harassment of Women Leaders: A review of the evidence." *VAWG Helpdesk Research Report.* No. 29. UKAID:Department of International Development.
Finnemore, Martha and Kathryn Sikkink. 2001. "Taking Stock: The Constructivist Research Program in International Relations and Comparative Politics." *Annual Review of Political Science* 4:391-416.
Greenberg, Andy. 2019. "Hacker Eva Galperin has a plan to eradicate stalkerware." *Wired*, March 3. https://www.wired.com/story/eva-galperin-stalkerware-kaspersky-antivirus/
Hafkin, Nancy and Sophie Huyer. 2007. "Women and gender in ICT statistics and indicators for development." *Information technologies and International Development* 4(2): 25-41.
Heller, Regina and Martin Kahl. 2013. "Tracing and understanding "bad" norm dynamics in counterterrorism: the current debates in IR research." *Critical Studies on Terrorism* 6(3):413-28.
Hu, Margaret. 2017. "Algorithmic Jim Crow." *Fordham Law Review* 86(2): 633-696
Smith, Chelsey. 2015. The Technology of Hope: Twitter and the #BringBackOurGirls Campaign." MA Thesis, Royal roads University, Victoria, British Columbia.
Htun, Mala and Francesca R. Jensenius. 2020. "Fighting Violence Against Women: Laws, Norms, and Challenges Ahead." *Daedalus* 149(1): 144-159.
Hudson, Valerie, Mary Caprioli, Bonnie Ballif-Spanvill, Rose McDermott, and Chad F. Emmett. 2009. "The Heart of the Matter: the Security of Women and the Security of States." *International Security* 33(3): 7-45.
Ibrahim, Dina. 2017. "Police-reported violence amongs same-sex intimate partners in Canada, 2009-2017.
Statistics Canada, March 20. https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00005-eng.htm).
(ISC)2. 2018. *Women in Cybersecurity: Young, Educated and Ready to Take Charge.* Florida: (ISC)2. https://www.isc2.org/Research/Women-in-Cybersecurity
Jee, Charlotte. 2019. "How "stalkerware" apps are letting abusive partners spy on their victims." *MIT Technology Review*, July 10. https://www.technologyreview.com/s/613915/stalkerware-apps-are-letting-abusive-partners-spy-on-their-victims/\
Katz, Andrew. 2017. *When Democracies Choose War: Politics, Public Opinion, and the Marketplace of Ideas.* Boulder: Lynne Reinner.
Kelly, Annie and Tina Johnson, eds. 2020. "Gender Equality: women's Rights in Review 25 Years After Beijing." UN WOMEN: Research and Data Section.
Kingston, Anne. 2019. "We are the dead." *Maclean's,* September 17. https://www.macleans.ca/news/canada/we-are-the-dead/.
Kimmel, Michael. 2018. "Almost all violent extremists share one thing: their gender." *The Guardian*, April 8.

https://www.theguardian.com/world/2018/apr/08/violent-extremists-share-one-thing-gender-michael-kimmel.
Khoo, Cynthia, Kate Robertson, and Ronald Diebert. 2019. *Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications.* Toronto: Citizen Lab at the Munk School of International Affairs.
Krook, Mona Lena and Julian Restrepo Sanin. 2016. "Violence against women in politics: a Defense of the concept." *Politics y gobierno* 23(2): 459-490.
Motherboard. 2019. "When spies come home: A multi-part investigative series about the powerful surveillance software ordinary people use to spy on their loved ones." *Motherboard,* https://www.vice.com/en_us/topic/when-spies-come-home.
Marche, Stephen. 2016. "Swallowing the Red Pill: a journey to the heart of modern misogyny." *The Guardian*, April 14. https://www.theguardian.com/technology/2016/apr/14/the-red-pill-reddit-modern-misogyny-manosphere-men.
Morgan, Steve. 2019. "Women represent 20 percent of the Global Cybersecurity Workforce in 2019." *Cybercrime Magazine*, March 28. https://cybersecurityventures.com/women-in-cybersecurity/.
Mother Jones News Team. 2014. "Women harassed out of their homes. Mass shooting threats. How #Gamergate morphed into a monster." *Mother Jones,* October 16. https://www.motherjones.com/media/2014/10/gamergate-explained/
Ndi, George. 2017. "Just in Bello: The IHL Principle of Distinction in the Context of Asymmetric and Irregular Warfare." In: 6th Annual International Conference on Law, Regulations and Public Policy, 5-6 June, 2017, Singapore.
Parashar, Swati. 2013. "What wars and 'war bodies' know about international relations." *Cambridge Review of International Affairs* 2013 26(4): 615-630.
Parsons, Christopher, Adam Molnar, Jakub Dalek, Jeffrey Knockel, Miles Kenyon, Bennett Haselton, Cynthia Khoo, and Ronald Deibert. 2019. *The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry.*Toronto: The Citizen Lab.
Peterson, Spike. 2005. "How (the meaning of) gender matters in political economy." *New Political Economy* 10(4): 499-521.
Piscopo, Jennifer. 2016. "State capacity, criminal justice, and political rights: Rethinking violence against women in politics." *Politica y gobierno* 23(2): 437-458.
Porter, Tony and Michael Webb. 2009. "The Role of the OECD in the Orchestration of Global Knowledge Networks." In *The OECD and Transnational Governance,* edited by Rianne Mahone and Stephen McBride, 43-60. Vancouver: UBC Press.
Powell, Anastasia, Adrian J. Scott, and Nicola Henry. 2018. "Digital harassment and abuse: Experience of sexuality and gender minority adults." *European Journal of Criminology*, 17(2): 199-223.
Public Safety Canada. 2018. "National Cyber Security Strategy." *Government of Canada,* May 28. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx.
Public Safety Canada. 2009. "National Strategy for Critical Infrastructure." *Government of Canada*, June 26. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx.

Risse-Kappen, Thomas, Stephen C Ropp, & Katheryn Sikkink. 2013. *The Persistent Power of Human Rights: From Commitment to Compliance*. Cambridge: Cambridge University Press.
Sadek, George. 2016. "Egypt: Sexual Violence Against Women." *the Law Library of Congress, Global Legal Research Center.* https://www.loc.gov/law/help/sexual-violence-against-women/egypt.php
Schoreder, Joanna. 2019. "Racists are recruiting. Watch your white sons." *The New York Times,* October 12. https://www.nytimes.com/2019/10/12/opinion/sunday/white-supremacist-recruitment.html
Shafqat, Narmeen and Ashraf Masood. 2016. "Comparative Analysis of Various National Cyber Security Strategies." *International Journal of Computer Science and Information Security* 14(1): 129-136.
Singh, Manish. 2020. "Indian police open case against hundred in Kashmir for using VPN." *Techcrunch*, February 18. https://techcrunch.com/2020/02/18/indian-police-open-case-against-hundreds-in-kashmir-for-using-vpn/?guccounter=1.
Sobieraj, Sarah. 2017. "Bitch, slut, skank, cunt: patterned resistance to women's visibility in digital publics." *Information, Communication & Society.* 21(11): 1-15.
Shahbaz, Adrian and Allie Funk. 2019. "The Crisis of Social Media: What was once a liberating technology has become a conduit for surveillance and electoral manipulation." *Freedom on the Net.* Washington, DC: Freedom House.
Shoker, Sarah. 2018. "Military-Age Males in U.S Counterinsurgency and Drone Warfare." PhD Dissertation, McMaster University.
Secretary-General. 2018. "Bridging the digital gender divide." OECD http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf
Shirazi, Farid, Ojelanki Negwenyama, Olga Morawczynski. 2010. "ICT expansion and the digital divide in democratic freedoms: An analysis of the impact of ICT expansion, education and ICT filtering on democracy." *Telematics and Informatics* 27:21-31.
Sjoberg, Laura. 2014. "Gender/Violence in Gendered/Violent World: Review Article." *Millennium: Journal of International Studies* 42(2): 532-542.
Sjoberg, Laura. 2011. "Gender, the State, and War Redux: Feminist International Relations across the 'Levels of Analysis.' *International Relations* 25(1): 108-134.
Sylvester, Christine. 2012. "War Experiences/War Practices/War Theory." Millennium, 40(3): 483-503.
Sorgner, Alina, Gloria Mayne, Judith Mariscal, Urvashi Aneja. 2018. "Bridging the Gender Digital Gap." *G20 Insights*, July 24. https://www.g20-insights.org/policy_briefs/bridging-the-gender-digital-gap/
Schmitt, Michael N. ed. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.
Taye, Berhan and Sage Cheng. 2019. "The state of internet shutdowns." *Access Now,* July 8. https://www.accessnow.org/the-state-of-internet-shutdowns-in-2018/
Taye, Berhan. 2019. "#IAMTHESUDANREVOLUTION: There's a direct link between internet shutdowns and human rights violations in Sudan!" *Acces Now*, June 11. https://www.accessnow.org/iamthesudanrevolution-theres-a-direct-link-between-internet-

shutdowns-and-human-rights-violations-in-sudan/
Walter, Ben. 2016. "The Securitization of development and humans' insecurity in Nangarhar Province, Afghanistan." *Global Change, Peace & Security* 28(3): 271-287.
UK Home Office. 2019. "Security summit ends with pledges to tackle emerging threats." *Gov.UK*, July 30. https://www.gov.uk/government/news/security-summit-ends-with-pledges-to-tackle-emerging-threats.
UN Internet Governance Forum. 2015. *Internet Governance Forum 2015: Best Practice Forum on Online Abuse and Gender-Based Violence Against Women Final Report*. Switzerland, Geneva. http://www.intgovforum.org/cms/documents/best-practice-forums/623-bpf-online-abuse-and-gbvagainst-women/file
UN Women. 2020. *Gender Equality: Women's Rights in Review 25 Years After Beijing.* New York, United States:Research and Data Section, UN Women.
UN Women. 1995. *Fourth World Conference on Women Beijing Declaration.* Beijing: UN Women. https://www.un.org/womenwatch/daw/beijing/platform/declar.htm.
UN Deputy Secretary-General, Amina Mohammed. 2018. "Better Laws, Data Essential for Tackling Cyberabuse, Growing Digital Gender Gap, Deput Secretary-General Tells Event on Ending Online violence against Women." *United Nations Meetings Coverage and Press Release*s, March 14. https://www.un.org/press/en/2018/dsgsm1142.doc.htm
UNESCO 2015. *Cyber Violence against Women and Girls.* UN Broadband Commission for Digital Development Working Group on Broadband and Gender.
Valentino-Devries, Jennifer. 2018. "Hundred of apps can empower stalkers to track their victims." *New York Times*, March 19. https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html.
Van Dijk, Jan A.G.M. 2013. "Digital Democracy: Vision and Reality." In *Public Administration in the Information Age: Revisited.* Edited by I. Snellen , Marcel Thaens, and W. van de Donk, 49-63. Washington, DC: IOS Press.
von Behr, Ines, Anais Reding, Charlie Edwards, Luke Gribbon. 2013. *Radicalisation in the digital era: The use of the internet in 15 cases of terrorism and extremism.* Brussels: RAND Europe. https://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR453/RAND_RR453.pdf
Wilkinson, Abi. 2016. "We need to talk about the online radicalisation of young, white men." *The Guardian*, November 15. https://www.theguardian.com/commentisfree/2016/nov/15/alt-right-manosphere-mainstream-politics-breitbart.
The White House. 2010. "National Security Strategy." *Washington*: The White House. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf
Whitworth, Sandra. 2004. *Men, Militarism & Peacekeepin*g. London: Lynne Rienner.
Woodhams, Samuel and Simon Migliano. 2020. "The global cost of Internet shutdowns in 2019." *Top10VPN*, January 7. https://www.top10vpn.com/cost-of-internet-shutdowns/
World Bank. 2012. World Development Report: Gender Equality and Development.

Washington:
The World Bank.
https://siteresources.worldbank.org/INTWDR2012/Resources/7778105-1299699968583/7786210-1315936222006/Complete-Report.pdf
Xiaoyu, Pu. 2012. "Socialisation as a Two-Way Process: Emerging Powers and The Diffusion of International Norms." *The Chinese Journal of International Politics* 5(1): 341-367.
Zaharia, Andra. "35+ initiatives to get more women into cybersecurity." *Comparitech*, March 17. https://www.comparitech.com/blog/information-security/women-cybersecurity-initiatives/.