ICTs, women's human rights and the WPS agenda

Conflict prevention and protection

Background

Human interaction in all its aspects has been radically transformed by the advent of digital technologies which now form an integral part of daily life. The benefits spawned by the technology have been enormous. ICTs have created new spaces of political engagement, promoted greater transparency and accountability, facilitated government and public sector efficiency, enhanced social empowerment through knowledge sharing, enabled greater access to education, healthcare and other social services and promoted economic empowerment through the creation of new industries, new relationships and new employment opportunities. But not all have benefitted. And in too many situations the technology has exacerbated existing inequalities, including gender inequalities.

Digital technologies have also unsettled long held assumptions which are only beginning to be understood, as are the legal implications thereof. For instance, it has collapsed traditional divides between the public and private, civilian and military, domestic and international; disrupted orthodox conceptions around time and space; and redistributed power and even redefined it thereby calling into question the role of the State and the interests it is expected to protect. Each of these disruptions – conceptual and material – and the fact that ICTs are transforming the nature of inter-State relations as well as the relations between the State and individuals has wide-ranging implications for international peace and security and for international law including women's human rights.

Much of the progress achieved through the Group of Governmental Experts (GGE) has largely concentrated on inter-State relations.[1] This is so both in respect of the general statements on how international law applies to the use of ICTs and to the identification of voluntary, non-binding, peacetime norms of State behaviour.[2] In a space that is becoming increasingly militarized, the need to re-affirm the legal obligations of States in their relations with each other is vital to maintaining peace and security. Yet, to focus primarily on the relations between States – defined by the interests of the most technologically advanced – is arguably to adopt a narrow and somewhat outdated conception of a pre-digital global order.

The creation of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security (OEWG) provides States with an opportunity to reflect on existing legal and policy approaches to digital technologies against the backdrop of a fundamentally transformed reality. The technology has already dispersed power. Individuals and groups with harmful intent are already taking advantage of a domain in which legally constructed borders have little traction. The private sector and civil society organisations are already crafting alternative governance models exemplified by the Cybersecurity Tech Accord, the Tor Project, the Citizen Evidence Lab, take back the tech project.

Gender, human security and ICTs

Both the GGE and OEWG are tasked with the study of "how international law applies to the use of information and communications technologies by States" which, by definition, includes international

[1] 2013 GGE report (A/68/98) and 2015 GGE report (A/70/174)

[2] A/70/174, 22 July 2015, paras 24, 28 and 13

human rights law and international humanitarian law.[3] To date, the GGE process has made little headway in delineating the scope and content of international human rights law in the cyber domain. The 2015 GGE report simply notes that "States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms" and "respect Human Rights Council resolutions 20/8 and 26/13" and "General Assembly resolution 68/167 and 69/166" on the right to privacy and freedom of expression.[4] In other words, what is emerging through the ICT discourse is the privileging of the conceptual distinction between State security and human security paralleling the international institutional divide that normalises and entrenches a separation. This siloed approach is problematic in that it enhances the risk of being blinded to and therefore failing to fully appreciate the linkages between peace and security and rights violations in the digital space. Moreover, it has also laid the foundations for States to develop and implement national cyber strategies that, at best, have inadvertently overlooked the human rights obligations of States and, at worst, simply dismissed them.

In a digital age, the human security lens provides States with a far more useful post-Westphalian analytic framework through which to conceptualise and craft policy and law.[5] However, what is typically missing from the human security discourse is the integration of a gender dimension. A gender perspective would assist in registering women's experience of insecurity in a digital age (which is often fundamentally different from that of men's experience) and surface harms otherwise ignored. For example, it would require us to ask how the exclusion and marginalisation of women from fully accessing, using, influencing and benefitting from digital technologies, on an equal footing with men, adversely and disproportionately affect women's ability to live free from fear or want, with an equal opportunity to enjoy all their rights and fully develop their human potential. The lack of commitment on the part of States to meet their fundamental human rights obligations is demonstrated by the gender digital divide – which in some regions is worsening – and further evidenced by the paucity of sex- and gender-disaggregated global data on ICT penetration. A gender sensitive perspective to human security would also assist in drawing linkages between different forms of insecurity including, for example, domestic violence and armed conflict or militarisation and violence against women.[6] In the context of ICTs, understanding the nexus between the rise in online violence against women and the growing tide of militarism is critical to combating both. Systematic human rights violations, including online VAW, do not occur in a vacuum.

UN Security Council's WPS Agenda and ICTs

The UNSC's WPS Agenda provides an entry point to assist States to craft policies pertinent to the cyber domain around a pre-existing framework that is designed to further peace and security and gender equality. Straddling four interlinking thematic pillars,[7] the transformative value of the WPS agenda lies in the fact that it requires States to adopt a *gender perspective* and *gender analysis*:

- to develop more nuanced understandings of what constitutes 'peace' and 'security';
- to identify the obstacles to peace and security;
- to craft policies to more effectively secure and maintain peace and security; and
- to interpret and apply international legal obligations.

[3] https://www.un.org/press/en/2018/gadis3619.doc.htm; https://ccdcoe.org/incyder-articles/a-surprising-turn-of-events-un-creates-two-working-groups-on-cyberspace/

[4] The GGE's 2015 report was adopted by consensus in General Assembly Resolution 70/237 (2015).

[5] See General Assembly resolution 66/290, 25 October 2012

[6] Chinkin and Kaldor, International Law and New Wars (2017) CUP, p 496

[7] The four pillars include: conflict prevention, protection, participation and relief & recovery. This note addresses only the first two pillars.

To understand how the WPS Agenda and the Resolutions[8] apply to ICTs, regard must be had to other supplementary materials including, for example, the UN's 2015 Global Study[9] and the contributions of the CEDAW Committee, most notably, General Recommendation 30 which engages specifically with the interplay between the WPS agenda and the Convention on the Elimination of Discrimination against Women [CEDAW].[10]

i) Conflict prevention

References to conflict prevention in the WPS Resolutions tend to focus on increasing women's role in decision-making.[11] Two decades after the adoption of SCR 1325, the participation of women in decision-making roles within international, regional and national institutions dedicated to conflict prevention diplomacy and mediation, military expenditure and disarmament remains troublingly low.[12] The failure by States to meet their policy objectives and legal obligations also represents lost opportunities to "design appropriate responses" to further conflict prevention including in the cyber domain.[13]

The need to include women in conflict prevention efforts, across all levels and within all institutions, formal and informal, is critical. However, the conflict prevention pillar is not exclusively concerned with women's participation. As noted above, it also requires a gender perspective to be applied to conflict prevention as an objective including in respect of operational measures to prevent violence and measures to address the root causes of conflict and violence. In short, what distinguishes the WPS framework from traditional approaches is that it calls for the adoption of a gender analysis in crafting such measures.

The potential for ICTs to advance conflict prevention both as a tool to enhance operational strategies and as a means to address the structural causes of conflict is expressly acknowledged in The Global Study. At the operational level, digital technologies can enhance the effectiveness of early warning systems through improved data gathering, collation and analysis although any additional benefit to women and girls will always turn on the extent to which gender has been integrated into developing the indicators themselves. That said, ICTs are already being piloted by States in conflict affected areas to register and flag increases in the level of risk to the security of civilian populations, including gender-based violence, enabling early non-violent targeted interventions.[14] Likewise, ICTs can enhance monitoring capabilities, including by civil society, that can help to direct early interventions to prevent violence and rights violations, especially in remote areas. Social media platforms are assisting knowledge sharing and risk awareness among and between communities that are at risk or have experienced violence.

---

[8] To date, the Security Council has adopted ten resolutions: 1325 (2000); 1820 (2008); 1888 (2009); 1889 (2009); 1960 (2010); 2106 (2013); 2122 (2013); 2242 (2015); 2467 (2019); and 2493 (2019).

[9] Preventing conflict, transforming justice, securing the peace: A Global Study on the Implementation of United Nations Security Council resolution 1325 (2015)

[10] CEDAW/C/GC/30, 18 October 2013. 189 States have ratified CEDAW. The SDGs and, in particular, Goals 5(b), 10 and 16 are also relevant but will not be addressed in this note.

[11] SCR 1325 (2000)

[12] The CEDAW Committee has repeatedly expressed concerns about women's exclusion from conflict prevention efforts; see General Recommendation 30, para 2.

[13] "It is only by including female stakeholders and using a gendered analysis of conflict that States parties can design appropriate responses", CEDAW Committee, General Recommendation 30, para 30

[14] General Recommendation 30, paras 29 & 33

ICTs can be further developed to tackle the structural causes of conflict and violence such as inequalities, weak governance institutions, corruption, the construction of violent masculinities and cultures of militarism among other factors. In requiring States to adopt a gender perspective, the WPS framework provides a particularly fruitful avenue for tackling the causes of conflict and violence which are typically rooted in and defined by gender norms, gender relations and gender inequalities. As the Global Study notes, "militarism and cultures of militarized masculinities create and sustain political decision-making where resorting to use of force becomes normalized mode of dispute resolution". [15] This is particularly pertinent to the cyber domain which is becoming increasingly militarized and unstable. The escalating frequency and intrusiveness of hostile cyber operations among and between the most technologically advanced States since 2012 indicates that far more resources are being channelled to developing ICTs as a method of controlling digital systems to disrupt, damage and/or destroy rather than addressing the structural causes of conflict and violence.

Through both national cyber strategies and WPS national action plans States should:

- ensure full, equal and meaningful participation of women in all conflict prevention institutions, formal and informal, from local to international;
- support the development and use of new technologies in the context of early warning systems ensuring that indicators are gender sensitive to enhance the security of women and girls whilst ensuring that such technologies do not inadvertently violate fundamental human rights;
- devise and implement educational and training programmes for men, women, boys and girls that reinforce and support non-violent, non-militarized expressions of masculinity both online and offline;
- promote strategies that nurture a culture of non-violent resolution of disagreement in both public and private spheres, online and offline;
- intensify efforts aimed at dispelling sexist attitudes and stereotypes offline and online.

ii) Protection

As with all technologies, ICTs can be developed and used to strengthen the protection of women and girls from all forms of violence. However, the reality is that women and girls often confront significant barriers rooted in pre-existing gender inequalities and discrimination that function to exclude them from accessing digital technologies in the first place. Common barriers include lack of education and language skills, scarce resources and secure spaces from which to access ICTs.[16] Moreover, in some communities, patriarchal socio-cultural norms are such that the male members of the household retain control over women and girls' access to the technology. In armed conflict there are further obstacles including power shortages, lack of dependable ICT infrastructure, forced displacement and the additional responsibilities that women and girls are required to take on that necessarily impinge on their time. For those who have access, ownership of a digital device, let alone use, can make them more visible thereby increasing their insecurity.

Although the advent of the mobile phone—the now dominant means of accessing internet in developing countries—was welcomed by many as a technological development that could mitigate some of the afore-mentioned barriers confronting women, the numbers convey a disappointing story. According to 2018 OECD figures, worldwide women are on average 26% less likely to have a

[15] Global Study, 207

[16] Worldwide, women and girls make up over half of those who are illiterate; see CEDAW General Recommendation 36 on the right of girls and women to education, 27 November 2017.

smartphone than men. In real terms, this translates to 327 million fewer women having smartphone access to the internet. In conflict and post-conflict situations the existing digital gender divide is likely to be greater.

Exclusion is already leaving many women less equipped to exercise their human rights and to benefit from the technology on an equal footing with men and, rather than being an empowering technology, ICTs are functioning to deepen inequalities in respect of a broad spectrum of rights.[17] Exclusion deprives many women and girls from accessing relevant and timely information around health and reproductive rights to enable them to exercise the right to access healthcare that, in some cases, may be a difference between life and death especially in conflict affected areas. Likewise, digital exclusion deprives women and girls from information that may be vital to accessing justice, participating in public affairs, securing shelter, food, among a whole host of other rights on an equal basis with men. For as long as women are excluded from access and use, they are less likely to be in a position to benefit from ICTs on a basis of equality with men let alone contribute to or influence the trajectory and content of this technology. Research is showing that digital technologies are legitimating and reproducing a gendered global order through the integration of gendered norms into the very design of digital technologies, including through algorithms and content.[18]

Policy reasons aside, States are under a legal obligation to address the gender digital divide given that it is rooted in and sustained by sex and gender-based discrimination.[19] Discrimination against women, as set forth in Article 1 of CEDAW constitutes:

> any distinction, exclusion or restriction made on the basis of sex which has the effect or purpose of impairing or nullifying the recognition, enjoyment or exercise by women, irrespective of their marital status, on a basis of equality of men and women, of human rights and fundamental freedoms in the political, economic, social, cultural, civil or any other field.[20]

Articles 2 and 3 of CEDAW require States parties to condemn all forms of discrimination and to take steps—legal and policy—to ensure that women and men enjoy equal rights *de jure* and *de facto* and, where appropriate, adopt temporary special measures in accordance with article 4 of the Convention. The obligation to ensure that women are able to access and use digital technologies on an equal basis with men may not be expressly stated in the treaty but is captured by the expansive definition of Article 1 and reaffirmed by the broad wording of Article 3 which requires States to take all appropriate measures to ensure the full enjoyment of rights on a basis of equality 'in all fields'.[21] Read together,

---

[17] https://www.elgaronline.com/abstract/journals/cilj/8-2/cilj.2019.02.02.xml

[18] https://blogs.lse.ac.uk/wps/2019/03/21/how-new-technologies-are-violating-womens-rights-in-saudi-arabia/

[19] The non-discrimination provision is contained in all main international regional human rights instruments and very many institutional human rights bodies have elaborated on the obligations of States to ensure that women are not discriminated against in the use of and access to digital technologies. For example, see Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights 'Standards for a Free, Open and Inclusive Internet' (15 March 2017) OEA/Ser L/V/II, CIDH/RELE/INF 17/17, section D

[20] Convention on the Elimination of All Forms of Discrimination Against Women (adopted 18 December 1979, entered into force 3 September 1981) 1249 UNTS 13 (CEDAW) art 1.

[21] Article 3 of CEDAW states, 'States Parties shall take in all fields, in particular in the political, social, economic and cultural fields, all appropriate measures, including legislation, to ensure the full development and advancement of women, for the purpose of guaranteeing them the exercise and enjoyment of human rights and

these two Articles anticipate the emergence of new forms of discrimination that may not have been identified at the time of drafting. Discrimination in respect of ICTs including through the digital technologies is clearly one such example. This obligation is an immediate one that must be read in conjunction with Article 24 requiring States to take all necessary measures at the national level to fully realised the rights in the Convention.[22]

The CEDAW Committee has emphasized on numerous occasions that discrimination can occur not only through the failure of States to take necessary legislative measures but the failure to adopt national policies aimed at achieving equality. It follows that in developing and implementing ICT policies and strategies States must assess the gendered impact of the proposed measures (including those already in place) and take concrete steps to formulate and implement policies targeted towards the goal of fully eliminating all forms of discrimination against women and achieving women's substantive equality with men.[23] The lack of available resources to invest in ICT infrastructure, or indeed the existence of an armed conflict, does not alleviate a state from its responsibility to ensure that women are not being disadvantaged from meaningful access and use by virtue of their sex/gender.

Over the years, the Committee has elaborated on what practical steps States should adopt to fulfil their Article 2 obligations stressing the importance of collecting sex-disaggregated data. Insofar as targeted temporary special measures are concerned, the Committee has repeatedly drawn attention to the need for States to pay special attention to those women belonging to disadvantaged and marginalised groups who confront/experience intersectional discrimination. For example, the Committee has emphasised the need for States parties to adopt special measures to improve the access to digital technologies by rural women and girls who are disproportionately disadvantaged due to the cascading layers of obstacles they face including poverty, geographic isolation, language barriers, lack of computer literacy and discriminatory gender stereotyping.

Article 2(e) of CEDAW requires States to take all appropriate measures to eliminate discrimination against women by any person, organization or enterprise. As the Committee has elaborated, States have a due diligence obligation to prevent discrimination by non-state actors. In practice this means that States must have in place effective policies, legislation, regulations and adjudication mechanisms to ensure compliance by private actors including all those operating in the ICT sector[24] and must engage all such actors and enlist their involvement in adopting measures that fulfil the goals of the Convention.

---

fundamental freedoms on a basis of equality with men'. See also General Recommendation No 28 on the Core Obligation of States Parties Under Article 2 of CEDAW' (16 December 2010) UN Doc CEDAW/C/GC/28, para 24.

[22] See also Articles 1(b) and 2(2) of International Covenant on Economic, Social and Cultural Rights

[23] In elaborating on the scope and content of Art 4 of CEDAW the CEDAW Committee has stressed that States parties are under an obligation 'to improve the de facto position of women through concrete and effective policies and programmes' and that States must 'address prevailing gender relations and the persistence of gender-based stereotypes that affect women not only through individual acts by individuals but also in law, and legal and societal structures and institutions'. Substantive equality, the Committee has emphasised 'calls for an effective strategy aimed at overcoming underrepresentation of women and a redistribution of resources and power between men and women'.

[24] The ICT sector ranges from start-ups to multinational corporations and includes (but is not limited to) all aspects of infrastructure, devices, networks and applications from telecommunication companies, network operators, equipment manufacturers.

The human rights implications of ICTs are complex and should not be understood as implicating only a handful of rights such as privacy and freedom of expression. Adopting a gender analysis reveals how States are failing to fully consider the gendered dimension of ICTs. This is so particularly in respect of addressing online violence against women. As the UN Special Rapporteur on Violence against Women notes, 'women and girls *across the world* have increasingly voiced their concern at harmful, sexist, misogynistic and violent content and behaviour online'.

The Security Council's recognition that women and girls experience violence on a "continuum" coupled with the fact that all violence is gendered, means that States should be crafting policies and law that are far more holistic in scope to address violence against women both online and offline.[25] While addressing conflict-related sexual violence (CRSV) has been at the forefront of the Council's attention pursuant to its WPS agenda, the Global Study concludes that *all* forms of violence against women and girls increase in armed conflict. Moreover, SCR 1325 expressly calls on 'all parties to armed conflict to take special measures to protect women and girls from gender-based violence … and all other forms of violence in situations of armed conflict'.[26] ICTs have given rise to new forms of violence against women – *the effects of which are tangible* – and, in too many cases, those who have been specifically targeted and threatened online have subsequently experienced physical violence and, in some cases, have been killed. Above all, women who have been able to amplify their voices most effectively through digital platforms be they human rights defenders, women in or running for public office, journalists and bloggers have been especially targeted.[27] In responding to the rise in targeted killings of women in leadership or public roles, including women's human rights defenders, the Security Council has called on states "to condemn acts of discrimination, harassment and violence against civil society" and "put in place measures to protect them and enable them to do their work" recognising that such persons are "important to changing norms on roots causes, namely structural gender inequality and discrimination".[28]

In emphasising that women's right to a life free from gender-based violence is indivisible from and interdependent of other human rights, the CEDAW Committee has regularly and frequently elaborated on the responsibility of States parties to prevent such violence and has provided detailed guidance on the measures that should be taken for States to fully comply with their obligations.[29] That States have an obligation to protect the same rights that exist offline in the digital sphere was affirmed by the UN Human Rights Council in 2016.[30] Yet, notwithstanding these commitments, domestic efforts to implement remain dismal at best. Few States have taken steps to enact domestic legislation to criminalise online VAW. The continued failure on the part of States to adequately respond to online misogynism and sexism is producing a culture in which women's subordination is normalised and institutionalised; in which threats and incitement to harm women is regularised; and in which physical and mental violence against women is tolerated.

Through both national cyber strategies and WPS national action plans States should:

---

[25] SCR 2467 (2019) preamble. The distinction between public and private violence, or indeed conflict and peacetime violence is a false distinction.
[26] Para 10.
[27] https://blogs.lse.ac.uk/wps/2017/11/27/why-addressing-online-violence-against-women-matters-to-the-wps-agenda/
[28] SCR 2467, para 21. See also Global Study, p73.
[29] General Recommendation No 35 (n 85) para 15.
[30] Human Rights Council 'The Promotion, Protection and Enjoyment of Human Rights on the Internet' (18 July 2016) UNGA Res 32/13, UN Doc A/HRC/RES/32/13.

- take positive and immediate steps including temporary special measures in accordance with their legal obligations to address the gender digital divide;
- collate gender disaggregated data on ICT access and use;
- remove discriminatory laws and regulations that impede full equality in accessing basic rights and services;
- adopt domestic legislation to criminalise all forms of gender-based violence against women, online and offline and ensure enforcement;
- introduce, without delay, or strengthen, legal sanctions commensurate with the gravity of the offence, as well as civil remedies;
- ensure that legal systems protect all victim/survivors and that they are able to access justice and are entitled to an effective remedy;
- eliminate the institutional practices and individual conduct and behaviour of public officials (in executive, legislative and judicial branches) that tolerate such violence or that provide a context for lack of a response or for a negligent response;
- adopt and implement measures to eradicate prejudices, stereotypes and practices, as set forth in Articles 2(f) and 5(a) of CEDAW; and
- provide additional support to women human rights defenders working offline and online.

Louise Arimatsu
December 2019