Gendering Cyberwarfare: Towards a Feminist Approach to the Development of International Humanitarian Law Applicable to Cyber Operations[1]

Tatiana Carvalho Teixeira

Abstract: The increasing use of information and communications technology (ICTs) for malicious purposes has triggered a debate about the role of International Law (IL) and International Humanitarian Law (IHL) in regulating cyberwarfare. This article stimulates the inclusion of a feminist perspective on the gendered aspects of conflict and how they can extend to cyberspace in the interplay between technology, conflict, and IHL.

Keywords: cyberwarfare; feminism; international humanitarian law.

Gênero na Guerra Cibernética: Rumo a uma abordagem feminista para o desenvolvimento do Direito Internacional Humanitário aplicável às Operações Cibernéticas

Resumo: O uso crescente de tecnologias de informação e comunicação (TIC) para fins maliciosos desencadeou um debate sobre o papel do Direito Internacional (DI) e do Direito Internacional Humanitário (DIH) na regulação da guerra cibernética. Este artigo estimula a inclusão de uma perspectiva feminista sobre os aspectos generificados do conflito e a sua possível extensão ao ciberespaço na interação entre tecnologia, conflito e o DIH.

Palavras-chave: guerra cibernética; feminismo; direito humanitário internacional.

1. The views expressed in this article are offered by the author in an individual capacity and do not necessarily reflect the official positions of the Ministry of Foreign Affairs of Brazil. The text is an excerpt from the author's Master's dissertation, defended at King's College London (Carvalho Teixeira 2023).

The overwhelming interconnectivity enabled by the development of information and communication technologies (ICTs) has affected virtually every aspect of human life, including conflict. Although cyberspace is predominantly used for civilian purposes, it is increasingly employed for malicious means by State and non-State actors (Sassòli 2019, 132), to the point that it has been classified as the "fifth domain" of warfare (Crowther 2017, 63). The securitization of cyberspace has ushered in a vivid debate aimed at exploring the different aspects of ICTs in conflict settings, including in the fields of International Law (IL) and International Humanitarian Law (IHL). Over the past two decades, scholars have grappled with several issues concerning the development of the laws of war regulating cyberwarfare.[2] The studies on the relationship between IHL and cyberwarfare, however, have steered away from exploring the nuances pointed out by feminist scholarship of the gendered aspects of conflict and how they could extrapolate to the cyber domain.

By choosing not to question gender neutrality, the current developments toward an IHL applicable to cyber operations are bound to replicate the same gender dynamics of traditional kinetic conflicts. The purpose of this article is to initiate a debate and stimulate a more comprehensive view of cyberwarfare that embraces a feminist perspective on the interplay between technology, conflict, and IHL. By asking the question "where are the women?" (Enloe 2000, 5) in cyberwarfare, it will seek to unpack the biases imbued in the concept of gender neutrality and the potential harms of transposing to cyberspace the gendered aspects pervading the highly masculinized and militarized law of armed conflict (LOAC).

This article is organized in the following structure: first, it will set out the theoretical framework upon which the research will be based; after briefly outlining the relationship between gender and IR and gender and IL, it will delve deeper into the feminist observations about the gendered aspects of IHL; then, the research will analyze two case studies of recent enterprises in developing IL and IHL applicable to cyber operations. The first case consists of the State-driven UN working groups in the field of ICT in the context of international security; the second is an academic exercise overseen by the North Atlantic Treaty Organization (NATO). Both processes will be assessed with a view to identifying the extent to which they

2. For the purposes of this article, cyberwarfare is defined as cyber operations conducted in or amounted to an armed conflict. The International Committee of the Red Cross (ICRC 2020, 483) defines them as ICT-reliant "operations against a computer, a computer system or network, or another connected device, through a data stream, when used as a means or method of warfare in the context of an armed conflict".

Tatiana Carvalho Teixeira *is a career diplomat and holds an MA in International Affairs with Specialism in Cyber Security (with Distinction) from King's College London.*

use gender as a category of analysis in their discussions. Finally, it will explore reasons and means for employing a feminist approach to the development of IHL applicable to cyberwarfare.

The idea of applying a gender lens to the development of IHL applicable to cyberwarfare stems from the realization that the literature on the subject has hitherto been centered mainly on two areas of study, namely the suitability of existing IHL to regulate cyberwarfare and, to those that believe the body of law can encompass cyberwar, the applicability and interpretation of the rules IHL to cyber operations. The first area assesses the difficulties in employing long-established rules of IHL (originally intended for physical confrontation) to hostilities involving new means and methods of warfare, such as cyber operations. A second area of study within the field consents to the application of existing IHL to cyber operations and turns to the ascertainment of *how* those rules could be applied. It focuses on analyzing the circumstances under which cyber operations could trigger IHL and the conditions necessary for the implementation of the regulations governing the conduct of hostilities, particularly the principles of distinction, proportionality, and precaution (Diamond 2014, 68).

The scholarship to date indicates that studies on the development of IHL applicable to cyber operations have steered away from including gender as a category of analysis in the process of regulating cyberwar. Most of the literature, however, echoes the ethnocentricity largely identified in the scholarship on international cybersecurity, adopting a positivist approach to the subject matter. Not only is the literature geographically and ideologically centered in the anglosphere, but it also largely fails to include perspectives from different epistemologies – such as gender, development, or critical studies – which could enrich the debate and help mitigate the perceived ethnocentrism.

What neither of these discussions considers is the possible gendered impacts of system impairments or destruction of civilian data, indicating a wide gap in the literature concerning feminist approaches to IHL and cyberwarfare. One of the few works making this connection to date was presented by Anwar Mhajne in an online

seminar. Examining some of Israeli's cyber-surveillance strategies against Palestinian activists, she adopts a feminist lens to argue for the need to include data protection and safe civilian access to ICTs under IHL. The gendered impacts of surveillance in a society ever more reliant on online communication have disproportionately affected women in the occupied territories, in what she regards as a violation of IHL (War Studies KCL 2022, 11:53-13:23).

The scholarship to date indicates that studies on the development of IHL applicable to cyber operations have steered away from including gender as a category of analysis in the process of regulating cyberwar. Most of the literature, however, echoes the ethnocentricity largely identified in the scholarship on international cybersecurity, adopting a positivist approach to the subject matter. Not only is the literature geographically and ideologically centered in the anglosphere, but it also largely fails to include perspectives from different epistemologies – such as gender, development, or critical studies – which could enrich the debate and help mitigate the perceived ethnocentrism. This article, therefore, seeks to address said gap in the development of IHL applicable to cyberwarfare by using a gender lens to assess the ongoing process of building up the rules that should govern cyber operations during armed conflict.

FEMINIST CRITIQUES TO IHL

Having underscored the scarcity of feminist analyses concerning the development of IHL applicable to cyber operations, it is important to scrutinize the contributions that feminist perspectives have provided to the development of IHL in general, starting with a brief rundown of the relationship between gender and International Relations (IR) and gender and law, before delving deeper into the interplay between gender and IHL. This framework will then provide the foundations for a feminist perspective to IHL applicable to cyber operations. It has been acknowledged that most of the scholarship to date hinges on an explanatory ontology and foundationalist epistemology of the subject matter. By adopting a feminist lens, this article wishes to shed a new light on supposedly neutral assumptions about the LOAC, cyberspace, and how they interact.

Inasmuch as feminist scholars propose an interpretive approach aimed at understanding events rather than explaining them (van Ingen 2016, 395), there can be not one but several different schools of feminism; similarly, the concept of gender is a contested one (Kinsella 2020, 145-59). Describing each feminist school and gender definition is beyond the scope of this article. However, it is important to clarify that, for the purposes of this research, gender is understood not in biological

terms, but as a social construction that constantly produces and reinforces the values, roles, and expectations attributed to different persons according to their labels (Richardson 2008, 19). Correspondingly, the feminist approaches underlying this analysis are not geared toward liberal equality nor professed in essentialist terms; rather, this essay perceives gender as having diverse meanings that are contextually and historically determined, and therefore should be assessed in its interrelationship with other factors of social differentiation, such as class and race.

Notwithstanding the differing definitions, most feminist scholars agree on the fact that gender intertwines with the concepts of masculinity, power hierarchies, patriarchy, and intersectionality. The application of these patriarchal hierarchies leads to a structure that values masculinity over femininity. It subjugates women to the dominance of men, and men with feminine attributes to other men deemed more masculine (Connell 2005, 74). Being a social construction, patriarchy's hegemony also pervades the field of International Relations; and although women played a foundational role in the development of the discipline in the early twentieth century, it was not until the 1980s that feminist IR came to be recognized as a school of thought in the field (Owens and Rietzler 2021, 1-8).

Feminist scholars in IR underscore the disregard of traditional foreign affairs writers for the fact that power in and among States strongly depends on sustaining notions about masculinity and femininity. They propose the inclusion of gender as a category of analysis in IR, with a view to both deconstructing the masculinist assumptions that permeate global politics (....) [and] the field of International Law. In this sense, feminist legal scholars seek to expose gender biases in an apparently neutral system of rules.

Feminist scholars in IR underscore the disregard of traditional foreign affairs writers for the fact that power in and among States strongly depends on sustaining notions about masculinity and femininity (Enloe 2000, 4). They propose the inclusion of gender as a category of analysis in IR, with a view to both deconstructing the masculinist assumptions that permeate global politics and proclaiming gender equality as a social goal (Tickner 1992, 8). By scrutinizing the public/private

dichotomy in the field of international relations, they unveil that not only are private affairs infused with patriarchal political structures but also that "the international is personal," meaning that national governments "depend on ideas of masculinized dignity and feminized sacrifice to sustain [their] sense of autonomous nationhood" (Enloe 2000, 196-197). Building on the notion of hegemonic masculinity, scholars such as J. Ann Tickner (1992, 58-59) posit a need to transform the concept of the "warrior-patriot" that has long depended on a devalued femininity and a militarized version of citizenship into the concept of the "citizen-defender".

The masculinist assumptions that permeate IR in general also pervade the field of International Law. In this sense, feminist legal scholars seek to expose gender biases in an apparently neutral system of rules. By asking "the woman question" (Gardam 1988, 266), they examine how the law usually fails to consider the experiences and values of women, or how legal standards and concepts tend to disadvantage them. Charlesworth et al. (1991, 634) spell out the contributions of feminist legal theory to the debate of IL in that it provides an interest, a focus of attention, a political agenda, a critical stance, an alternative method of practicing, and, most importantly, a means of reinterpreting and reformulating International Law so that it more adequately reflects the experiences of all people.

Feminist legal theorists call into question the myths of neutrality and universality of International Law. Unlike what many Western theories proclaim, the law is not an autonomous entity, disassociated from the society it aims to regulate; it is a socially constructed system of beliefs, and its analysis cannot be separated from the political, economic, historical, and cultural context from which it stems. Therefore, there can hardly be any neutrality or objectivity in the law. To feminist scholars, the concept of gender neutrality comes from unequal starting points. They highlight the importance of making laws that are "substantively equal," since equality as a mere tool can be proven unjust when applied to situations where disparities exist (Stern 2019, 89). As it currently is, "International Law is a thoroughly gendered system" that works to perpetuate the dominance of masculinity over femininity. States, the primary subjects of International Law, reflect patriarchal structures, and the traditional principles of international law, such as sovereign equality, territorial integrity, and political independence, reinforce this patriarchal system and relegate women's concerns to an inferior category, the "private" sphere in the public/private dichotomy. Such an excessive focus on States obscures the fact that the impact of the law will be felt the most at the individual level, not by the abstract entity (Charlesworth et al. 1991, 614).

Having briefly outlined some of the feminist contributions to international relations and international law, it is time to scrutinize the interplay between

feminism and IHL, a field regarded by gender scholars as the "quintessential male arena" (Stern 2019, 87). The realm of armed conflict is fraught with stereotypes and socially constructed expectations about men and women. Gender stereotypes about weakness and vulnerability lead to an emphasis on the protection of women in conflict, despite the fact that men have a much higher risk of being directly targeted. Conversely, masculinity underlies militarism and the war-making endeavor (Stern 2019, 86), in a misleading association between men and violence that relies not on an innate aggressiveness, but on the "construction of a gendered identity that places heavy pressure on soldiers to prove themselves as men" (Tickner 1992, 40). This highly gendered environment is echoed in the body of law that regulates it. IHL conventions were drafted predominantly by male negotiators, leading to an international legal order that reflects a masculinized perspective of conflict (Charlesworth et al. 1991, 644). Moreover, the relegation of women to the private sphere results in their alienation from the decision-making process in "the most public and powerful function of the State: the use of force" (Gardam 1988, 277).

Especially in the case of IHL, feminist scholars question the universality of the law. The LOAC is not only androcentric but also Eurocentric, having assimilated Western legal ideas, including the patriarchal belief that the law can be objective, gender-neutral, and universally applicable (Charlesworth et al. 1991, 644). In practice, when scholars refer to IHL they mean the law regulating traditional armed conflict between Western States, since this body of law was developed having the experience of European States as its basis for the legal regime. And inasmuch as IHL is predicated on certain cultural assumptions, it is met with mixed success when confronted with conflicts involving non-European States; therefore, a feminist approach to IHL must confront not only gender specificity but also cultural specificity (Gardam 1997, 68-69).

When scholars refer to IHL they mean the law regulating traditional armed conflict between Western States (...). And inasmuch as IHL is predicated on certain cultural assumptions, it is met with mixed success when confronted with conflicts involving non-European States; therefore, a feminist approach to IHL must confront not only gender specificity but also cultural specificity.

Feminist critiques of IHL in general highlight the law's gendered origins hence its resulting reductionist approach to gender (Stern 2019, 99). The 1949 Geneva Conventions (GC) were inspired by the thoughts of Hugo Grotius, who believed women should be spared in conflict as they supposedly lacked the capacity to devise war (Grotius 1625). Consequently, "gender is reduced to women, women are reduced to victims, and female victims are reduced to sexual violence" (Stern 2019, 103). Such a narrow approach is detrimental not only to women but to all involved. By focusing on the protection of women rather than on the prohibition of violence, the law fails to acknowledge that men are also victims of sexual violence in wartime and thus also in need of protection; it also fails to address the use of sexual violence against men in war as a strategy to humiliate and emasculate them, pushing them to the bottom of a power structure based on gender stereotypes. The adoption of a gender perspective to IHL is a reminder that the debate is not a contest between mutually exclusive concepts (Durham and O'Byrne 2010, 48-49).

Furthermore, IHL's reductionist view of gender leads to provisions that are of limited use, since women are protected only as performers of specific roles, such as mother, child-bearer, or wife. Of the 34 GC provisions ostensibly safeguarding women, 19 of them are actually intended primarily to protect children (Gardam 1997, 57). Sexual violence against women is not regarded by the GC as an offense on them per se but is rather perceived as an attack on their honor, implying protection not of themselves but of their husbands and fathers. Such gendered conditions lead to Helen Kinsella's (2004, 2) warning about the risk of perpetuating inequalities due to the mutually reinforcing role of law in shaping society and vice-versa, since these provisions "focus primarily on the *protection* of women within the law rather than on the *production* of women in the law."

Another feminist critique of IHL hinges on the aforementioned myth of neutrality, which conceals the gender hierarchy implicit in the LOAC. It has already been established that a formally equal system of law can hardly achieve substantially equal results, given the inherent inequalities and the different ways men and women are affected by conflict. In the case of IHL, the binaries exposed by feminists are more flagrant, with the public/private paving the way for the combatant/civilian, military/civil, and protector/protected, in which the interests of the former, associated with the masculine, are favored over those of the latter, linked to the feminine (Stern 2019, 104). Thus, in the LOAC, women suffer a "double disability" in comparison with combatants: "their status and treatment are not only inferior as civilians but doubly so as women civilians" (Gardam 1997, 64).

Finally, the gendered nature of IHL is also evident in the application of the law's guiding principles of humanity and distinction, which must always be reconciled with

the principles of proportionality and military necessity (Gardam 1988, 276). To feminist scholars, it is difficult to calculate unlike phenomena and compare anticipated events, especially since proportionality calculations are usually made in terms of casualties, whilst women tend to be targeted in different ways, such as sexual violence, displacement, and loss of infrastructure. They also argue that the laws of war have been formulated deliberately to privilege military necessity at the cost of humanitarian values, by assuming that war is inevitable, and soldiers are performing a necessary, thankless duty to protect society – and society's women (Gardam 1997, 72).

The process of developing international law applicable to cyber operations must take into account the contributions of feminist approaches to IHL, lest it could repeat and reinforce the unfair gender dynamics already entrenched in the body of law regulating kinetic warfare.

The feminist critiques of IHL have demonstrated that "conflicts are gendered spaces" and that the law can be instrumental in perpetuating unfair gender dynamics (Stern 2019, 86-87). Both the structure of international law-making and the content of the rules of the LOAC privilege masculinities, leaving women's concerns either marginalized or blatantly dismissed (Charlesworth et al, 614). Therefore, the importance and usefulness of using gender as a category of analysis in IHL are that it can "open up discussion on the construction of social rules that impact upon communities, and how these roles can and do change" (Durham and O'Byrne 2010, 34). Applying a gender perspective on IHL can strengthen the protection to all that are in a position of vulnerability – combatants or civilians, regardless of gender – in armed conflict.

With the ever-increasing securitization of cyberspace comes the need to forge rules that regulate hostilities in this new, rather uncharted domain of warfare. The process of developing international law applicable to cyber operations must take into account the contributions of feminist approaches to IHL, lest it could repeat and reinforce the unfair gender dynamics already entrenched in the body of law regulating kinetic warfare.

Having set out the theoretical framework under which feminist scholars view the LOAC, this article now turns to an analysis of two ongoing processes of developing international humanitarian law pertinent to cyber operations. It will scrutinize two case studies that embody institutional and informal processes of international law-making and assess the extent to which these processes have included gender as a category of analysis in their considerations.

DEVELOPING IHL APPLICABLE TO CYBER OPERATIONS: CASE STUDIES

As noted by the mainstream literature on the subject, there is divergence both in scholarship and among States over the most suitable method for advancing International Humanitarian Law applicable to cyber operations. The contention lies in the methodological choice to be made regarding IHL rules in cyberwarfare. Two approaches are put forward, namely, a *methodological* approach that focuses on the interpretation of existing rules of the LOAC, and an *evolutionary* approach that seeks to inherit the key values of IHL while adapting the *jus in bello* to the specific features of cyberspace (Delerue and Yang 2023, 11-12).

For over two decades, there has been discussion about the need for a new treaty to regulate conflicts in cyberspace. The Russian Federation has advocated for a new treaty since the 1990s, and alongside China takes the position that a treaty regime to govern cyberspace is a better approach than relying on customary law and non-cyber-specific treaties (Schmitt 2021, 666). Conversely, the U.S. and Western States argue that the current international atmosphere does not favor new treaties in this field (Sassòli 2019, 542), and that the existing rules of IHL sufficiently address the issues raised by new means and methods of warfare such as cyberweapons (Droege 2012, 535). These controversies are imbued in a context of not only great power narrative disputes (Hansel 2023, 1-2), but, most importantly, of a deliberate position of "strategic ambiguity" and a silent arms race (Moyninhan 2021, 398; Sassòli 2019, 535).

In light of the current stalemate on a formal treaty negotiation to advance laws regulating cyber operations in conflict, actors have resorted to alternative methods to develop IHL applicable to cyberwarfare. These processes encompass either the establishment of voluntary, non-binding norms negotiated by States under the framework of a multilateral organization or attempts at "informal international law-making" (IIL), an alternative already being employed to advance other aspects of IHL pertaining to kinetic warfare (Janssens and Wouters 2022, 920-21). The two case studies presented in this article illustrate each respective process. The following section will scrutinize each of these pathways and analyze the extent to which they address gendered aspects of cyberwar.

Institutional processes: the United Nations GGEs and OEWG

Since the first request for an international resolution on the application of ICT technologies in the context of international peace and security back in 1999 (UN Doc A/C.1/53/3), the United Nations has witnessed increasing interest –

and contention – in the subject. In 2003, the General Assembly tasked a group of governmental experts (GGE) with analyzing international cyber threats (UN Doc A/60/202). In the past twenty years, six GGEs have been convened to engage in discussions that range from norms of responsible State behavior and application of IL and IHL, to the establishment of confidence-building measures and capacity-building initiatives (UNODA 2019).

The specific discussions around IHL and cyberwarfare gained momentum in the aftermath of the 2008 conflict between Russia and Georgia, where cyber operations were employed in the hostilities (Schmitt 2021, 663). In 2013, the GGE consensus report acknowledged that "international law, and in particular the [UN] Charter, is applicable and is essential" to maintaining peace (UN Doc A/68/98). Two years later, the 2015 GGE report made significant progress by agreeing on eleven voluntary norms of responsible State behavior in cyberspace (UN Doc A/70/174). It noted the humanitarian principles of "humanity, necessity, proportionality, and distinction," even though it did not directly use the term *international humanitarian law*. This very term would be the bone of contention that eventually led to the fifth GGE's failure to reach a consensus report (Schmitt 2021, 664). Russia, China, and Cuba objected to the inclusion of the term, on the grounds that explicit reference to IHL "would legitimize a scenario of war and military actions in the context of ICT" (Rodríguez 2017).

Arguments against the militarization of the internet notwithstanding, the sixth GGE accomplished a compromise (Mačák 2021, 411-12). Whilst admitting the need for further study on the subject, its consensus report in 2021 (UN Doc A/76/135) explicitly stated that "International Humanitarian Law applies only in situations of armed conflict," recalled the principles noted in 2015, and posited that "recalling these principles by no means legitimizes or encourages conflict."

Amid the 2017 GGE failure and the criticism towards the group's composition structure, some States led by Russia put forward an Open-Ended Working Group, in parallel with the sixth GGE and also under the auspices of the General Assembly, to discuss the same issues. Both groups operate on the basis of consensus; however, whilst the GGEs have limited membership and meet behind closed doors – which is argued to enjoy the benefit of greater efficiency in meeting consensus – (Schmitt 2021, 677), the OEWG was designed as an inclusive and transparent process, even allowing some degree of participation of non-State parties. Nevertheless, the OEWG final report in 2021 did not make direct reference to IHL. The deadlock was evident in the group's Chair Summary, which conceded that "discussions on the applicability of [IHL] to the use of ICTs by States needed to be approached with prudence" and that "further study was required" (A/AC.290/2021/CRP.3).

Whilst fractured, the discussions at the UN are commendable for conveying a positive degree of engagement in what seems an increasingly transparent, inclusive, and global process. The broad debate establishes important building blocks that can support the development of cyber-specific understandings of IL and IHL (Moynihan 2021, 395). Even though the reports are considered non-binding norms, it is expected that some of these understandings may eventually be recognized as law or even crystallize into customary International Law or authoritative interpretations on existing rules (Schmitt 2021).

Having outlined the main discussions within the UN concerning the development of IHL applicable to cyber operations, we now analyze the extent to which the GGE and OEWG processes included, whether in form or in substance, feminist considerations about the possible gendered impacts of conflict in cyberspace.

In terms of composition, cyber diplomacy remains male-dominated, following a recurrent pattern of arms control and disarmament diplomacy. Even though the average proportion of women slowly increased through each session, on average they represented but 20.2% of delegates. The OEWG has slightly improved figures, with women amounting to 32% of delegates, even though only 24% held leadership positions (UNIDIR 2019). It is important to highlight, however, that the increasing participation of women can be attributable to a broader-ranging institutional policy at the UN. The Secretary General's Agenda for Disarmament, established in 2018, included a commitment to achieve gender parity on all panels and groups created under his auspices in the field of disarmament (UNSG 2018).

In terms of content, the discussions and outcomes remain masculinized and highly securitized, although there has been some progress in the past few years. The reports adopted by the GGEs in 2010, 2013, and 2015 are silent about gender, women or girls. They only go as far as mentioning a need to respect "human rights and fundamental freedoms" and "privacy and freedom of expression," but fall short of exploring the potential gendered harms emerging from the design and utilization of ICTs (UN Doc A/65/201; UN Doc A/68/98; and UN Doc A/70/174). The atmosphere started to change in the 2019-2021 GGE, whose consensus report makes a brief reference to gender within the norm of respecting digital human rights, stating that the observation of said norm could "contribute to promoting non-discrimination and narrowing the digital divide, including with regard to gender" (UN Doc A/76/135). The OEWG went further: acknowledging the prominence of gender perspectives throughout the discussions, the group's final report underscored the importance of "narrowing the 'gender digital divide' and of promoting the effective and meaningful participation and leadership of women." It also recommended that capacity-building initiatives be "gender-sensitive, inclusive and non-discriminatory"

(UN Doc A/AC.290/2021/CRP.2). Moreover, throughout the OEWG sessions, delegations and external observers made statements and submitted working papers not only proposing that gender equality and the meaningful participation of women be at the center of the discussions, but also stressing the need to adopt a gender lens to the issues of ICT and international peace and security (Sharland et al. 2021, 17).

The language incorporated into the 2021 OEWG Final Report and Chair's Summary demonstrates perhaps the most substantive progress hitherto within the UN to include feminist approaches into the international cybersecurity agenda, including the need to integrate gender perspectives (Sharland et al. 2021, 18). The fact that most advancements took place under the OEWG rather than the GGEs may be an indicator that the structure of the former, which favors transparency and inclusivity, may better contribute to the inclusion of gender as a category of analysis in the evolving discussions on the applicability of IL and IHL to cyberspace. The limited pace of progress and high level of controversy specifically towards the development of IHL, however, suggests that formal processes may struggle to meet the challenges posed by the ever-increasing impacts of cyber technologies. The next section will address alternative pathways to develop rules of war aimed at regulating cyber operations.

Informal attempts at international law-making: the Tallinn Manuals

The perceived difficulties in advancing formal rules of IHL to regulate cyber operations during armed conflict have led some scholars to argue for the resort to tools that extrapolate the traditional sources of international law inscribed in Article 38(1) of the Statute of the International Court of Justice (ICJ) as "the only way forward to meaningfully develop IHL". According to its advocates, the concept of "informal international law-making" would be an alternative to break the deadlock in negotiations by vesting a degree of informality whether in the process, in the actors involved, or in the output of the enterprise (Janssens and Wouters 2022, 2114). Given the gendered nature of conventional law-making processes and outcomes, on a first sight the prospects of adopting IIL to cyberwarfare would present an opportunity to bring different perspectives to the table and achieve more balanced results. Nevertheless, the most notable IIL exercise hitherto performed, The Tallinn Manuals on the International Law Applicable to Cyber Operations (Schmitt 2017), has fallen short of addressing the gender silence on IHL, as will be demonstrated below.

The Tallinn Manual is a remarkable academic study conducted by legal experts at the invitation of NATO's Cooperative Cyber Defense Center of Excellence (CCDCOE) in the aftermath of the 2007 cyber-attacks in Estonia

(Lucas 2016, 64-65). The members of the "International Group of Experts" (IGE) were invited in their personal capacity to examine how extant legal norms, particularly of IHL, would apply to cyberwarfare. Its first edition focused solely on the aspects within the *just ad bellum* and the *jus in bello* contexts, while the second edition extended the scope to include an assessment of International Law applicable to peacetime operations (Schmitt 2017, 1-3). In order to persuade the global community of its authority, the Manual is presented not as a law-making project but as a mere interpretation of already existing rules of International Law, "an objective restatement of the *lex lata*" (Shereshevsky 2022, 2147). It also claims to be "policy and politics-neutral," underscoring the independence of the experts from their institutions and States of origin, the nations that sponsored the project, and NATO's CCDCOE (Schmitt 2017, 3).

The Tallinn Manual is a solid professional exercise in that it provides contributions to the legal debate on issues of utmost importance, such as the diverging understandings of the meaning of "attacks" in cyberspace, and the extent to which civilian data can be protected as *civilian objects* under IHL. Its effort, however, comes with an approach that intentionally perceives cyber operations as an analogy of physical military operations, adopting a sort of "kinetic equivalence effects test" (Biggio 2017, 44). Formidable as it is, it fails to explore the transformative impacts of technology upon the global security environment, challenging the threshold between the physical and digital worlds and the binary parameters of war and peace (Kello 2017, 77-78). Furthermore, the Manual's claims of neutrality and objectivity conceal several gender-based assumptions, both in its content and in its form.

In terms of its substance, the Tallinn Manual abides by the traditional conceptions of IHL. It is centered mostly on the Western image of statehood, failing to address the increased leverage held by private institutions and individuals in cyberspace. The Manual's 154 "black letter rules" and commentaries seem to have been written under the public/private dichotomies and the gendered hierarchy attributed to combatants over civilians. As already mentioned, the notions of "attack" and "civilian objects" follow a misleading equivalence to kinetic warfare. Moreover, the Manual is virtually silent on aspects of sex or gender-based violence. The sole mention of gender is made in the commentaries to rule 146 about the respect for protected persons in occupied territory, which states that "subject to special provisions related to health, age, and gender," the occupying power must afford the same consideration to protected persons, "without any adverse distinction based, in particular, on race, religion, or political opinion" (Schmitt 2017, 544-45). In its substance, therefore, the Manual is but a reflection of the gendered system of IHL.

Perhaps the main reason for the gendered substance of the Tallinn Manual lies in its form and drafting process. All members of the IGE in the first edition – the one which mainly analyzed the application of IHL to cyberspace – came from Western countries (Schmitt 2017, xix-xxii), even though at the time there had already been other States affected by and involved in cyber operations, such as Russia, China, Iran and Israel (Tanodomdej 2019, 75). Moreover, the Manual's drafters resorted to the national military manuals of Canada, Germany, the United Kingdom, and the United States as reference materials to their work, thus reinforcing the perception that the resulting document could channel, even if it would not officially represent, a specific worldview towards IHL (Eichensehr 2014, 588). In a lecture at Harvard University, the director of the project, Professor Michael N. Schmitt, explained the selection process:

> *How did we do it? We brought 20 experts from around the world, a very politically incorrect group of experts, because we knew we were doing this for the first time, so we really didn't care if we had geographical distribution etc. We took the 20 best people we could find. […] And then there were three advisers: one from the United States Cyber Command […]; an International Committee of the Red Cross representative […]; and then we had a representative from NATO, primarily because NATO provided us the cash for the project, and if you give us money you get a seat at the table (HLS Program 2015, 14:20-16:56).*

What seems most problematic about the drafting process of the Tallinn Manual is not so much that it concentrates on the views of Western countries on the application of IHL to cyber operations, but that it attempts to assert that the resulting document represents the views of the international community as a whole (Tanodomdej 2019, 76; Fleck 2013, 335). The Manual's alleged authoritative degree has been met with hesitancy by non-Western scholars and State representatives, and implementation of its rules is usually limited to the list of countries from which the experts came (Janssens and Wouters 2022, 2130).

In the wake of the intense criticism generated by the limited diversity of participants and the heavy reliance on Western legal sources, the second edition of the Tallinn Manual attempted to address these shortcomings by inviting a wider group of experts and hosting a consultation process with 50 States. Published in 2017, Tallinn Manual 2.0 still relied heavily on the positions of Western, male, military-based scholarship (Schmitt 2017, xii-xviii). A third attempt was initiated in 2021, with the broader purpose of addressing "the evolving nature of cyber

operations and State responses" (CCDCOE 2023a), and the adoption of an online crowdsourcing tool to receive contributions from any expert interested in the topic, in order to ensure that the final document "reflects all reasonable views" (CCDCOE 2023b). In an interview about the drafting process of Tallinn 3.0, project director Michael N. Schmitt stated that "representative of 'specially affected States' is not a definitive criterion we will be using (…), although we do want representations from certain key players in cyberspace" (Dunlap 2021).

The experience of the Tallinn Manuals indicates the opportunities and shortcomings of informal international law-making. The Manual provides the reader with a thorough interpretation of the IHL norms applicable to cyber operations. It can prove valuable in the process of scrutinizing the extent to which existing norms can regulate the application of cyber technologies in warfare, with the caveat that said interpretations follow a traditional, State-centric approach to IHL that overlooks the gendered nature of conflict itself. That achievement notwithstanding, the Manual cannot claim to represent an authoritative global view on the subject, inasmuch as it reflects the understandings of a very specific set of States, and can disguise underlying political agendas (Tanodomdej 2019, 73). However easier it may seem to negotiate with like-minded countries, only by achieving a truly global understanding of acceptable behavior in cyberspace can the rules governing cyber conflict be followed (Eichensehr 2014, 588).

TOWARDS A FEMINIST PERSPECTIVE ON IHL AND CYBER OPERATIONS

Having assessed the two main processes currently in place to develop regulations applicable to international cyberwarfare – and the extent to which they help reproduce or subvert traditional gender dynamics in war – it is time to analyze why and how a feminist perspective on cyber operations can contribute to constructing a more inclusive and just body of law for IHL in the digital age.

The adoption of a gender lens to the process of regulating cyberwarfare is important because, just as there can be no gender neutrality in the law, technologies are not neutral; they are imbued with the political values and objectives of those who create them (Devidal 2023). This is why some female scholars champion the inclusion of gender-related considerations in as early as the study and development phases of new technologies of war, when carrying out the legal review of these new means and methods of warfare prescribed by article 36 of the Additional Protocol I to the GC (Farrés Jiménez 2022). From the very beginning, stakeholders and decision-makers who need to apply IHL ought to understand how gender factors might

impact the use of the code weapon and the application of the law.

The gendered repercussions of the anonymity and accessibility provided by cyber technologies have already been identified in the broader field of cybersecurity. These include, but are not limited to, a disproportionate exposure of women to cyberstalking, online harassment, non-consensual dissemination of information, online violent extremism and trafficking, as well as targeted disinformation campaigns (Sharland et al. 2021, 2). In the case of cyberwarfare, there is not as much evidence to work with, not only because the world has not witnessed as many armed conflicts involving the deployment of cyberweapons,[3] but chiefly because cyber technologies stretch traditional IHL tenets to such an extent that they also transform the gender dynamics imbued in physical conflict.

The adoption of a gender lens to the process of regulating cyberwarfare is important because, just as there can be no gender neutrality in the law, technologies are not neutral; they are imbued with the political values and objectives of those who create them.

Observing cyberwarfare through a feminist lens is also a helpful tool to question the assumptions embedded in mainstream discourses. A gender perspective can help deconstruct the myth that cyberweapons are ethically superior to physical arms due to their relative non-lethality (Droege 2012, 574). Claiming that cyber operations cause less incidental damage to civilians or civilian infrastructure than kinetic attacks overlooks the fact that mortality is not the only metric in warfare, and people can be severely harmed without being killed or physically injured (Rowe 2015, 308-09). Moreover, it is already known that the direct effects of a cyber-attack – damage to a computer – are usually less significant than its indirect effects – damage to a system connected to a computer (Lin 2012, 519). And it is precisely the indirect effects of war that disproportionately impact women; the higher protection of their bodies from deadly attacks does not shield them from the heavier economic, social, and cultural hardships of conflict and post-conflict environments (Gardam 1997, 60).

The idea that cyber operations would be less harmful in war carries within it the controversial discussion about the dehumanization of warfare. Code wars entail further distancing between the attacker and the victims, creating more opportunities for errors and misjudgments and a greater risk of collateral and persistent damage.

3. For emerging studies about the cyber dimensions of the armed conflict in Ukraine, see https://cyberpeaceinstitute.org/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q4-2022/.

This increased distance from the battlefield will eventually target more civilians than the military, and we have already established earlier in this article the gendered quality of the civilian/military dichotomy (Rowe 2015, 325). Moreover, due to the significant imbalance in military capabilities and technologies between the West and the Global South, the gendered consequences of cyber-attacks are bound to intersect with race, class, and other factors, thus widening global asymmetries.

The idea that cyber operations would be less harmful in war carries within it the controversial discussion about the dehumanization of warfare. (...) Moreover, due to the significant imbalance in military capabilities and technologies between the West and the Global South, the gendered consequences of cyber-attacks are bound to intersect with race, class, and other factors, thus widening global asymmetries.

Analyzing the interplay between humanity and technology in the context of war, some feminists go as far as calling for a "*posthuman*itarian international law". According to these scholars, we already live in a posthuman condition where "the human is always-already digital and material; it is already more-than-human" (Arvidsson 2018, 13). We already have digital bodies, and these bodies do not perform one or other gender, i.e., in the digital realm, gender entangles but cannot be conflated with our material bodies. The lives in contemporary high-tech warfare go far beyond the conventional bodies envisioned through IHL's binary-gendered distinction. Therefore, digital war affects the more-than-human in ways that current IHL cannot grasp. What we experience in cyberwarfare is not less violence but rather "new and other forms of violence" (Arvidsson 2018, 18-19; 27). The complexity of this novel context needs to be taken into account in the process of developing laws to regulate cyber conflict, otherwise it risks perpetuating or even exacerbating unfair dynamics.

What underlies these unequal circumstances is the realism-based, hypermilitarized approach to IHL (Tickner 1992, 128), which privileges masculine characteristics and imposes a hierarchy of values that favors the State-centric aspects of conflict to the detriment of human rights and humanitarian considerations. In no other branch of International Law does an institution with so many vested interests such as the military exert so much influence as in IHL

(Gardam 1997, 62). The case studies analyzed in this research indicate that this hierarchical structure is being reproduced in the discussions about operations in cyberspace. The fact that the topic of cybersecurity is undertaken within the UN arms control and disarmament bodies, together with the high number of retired military officers participating in the Tallinn Manuals IGE (Schmitt 2017, xix-xxii), contributes to perpetuate this masculinized slant. Including gender and other social factors as categories of analysis can encourage research that brings a human face and dimension to the study and discussion about cyberwarfare (Pytlak 2020, 68).

Inasmuch as gender biases affect the processes of developing technology and developing law, in the masculinized warfare environment these biases are likely to be aggravated. This is why feminist scholars advocate for gendering the legal review of new means and methods of warfare. A feminist perspective is useful to question assumptions of a higher "humanity" within cyberwar, especially when the very idea of "human" acquires new layers in cyberspace. Whether cyberwarfare is just a continuation of conflict by other means or an entire novel phenomenon, a feminist lens can help keep track of gender inequalities and propose more inclusive and equitable pathways.

CONCLUDING REMARKS

One of Simone de Beauvoir's most famous quotes reads that "representation of the world, like the world itself, is the work of men; they describe it from their own point of view, which they confuse with absolute truth" (Beauvoir 2000, 235). Her assessment is a fitting illustration of the laws that regulate warfare, which reflect a masculinized and highly militarized view of conflict. Although the international law of cybersecurity is still in a "state of infancy" (Schmitt 2021, 661), it is already on a path to reproducing the same unequal gender dynamics that permeate traditional IHL.

This article has sought to explore the possible contributions of feminist scholarship to the process of developing international humanitarian law applicable to cyberwarfare. Having identified a gap in the literature around the subject, it resorted to feminist IR and feminist legal theory to bring to light some of the gendered aspects of traditional IHL. It underscores how seemingly neutral principles of the *jus in bello* conceal built-in gender stereotypes that favor a masculinized approach to warfare, reducing women to victimized roles. Feminist contributions to IHL have demonstrated that the law can be instrumental in perpetuating unfair gender dynamics, privileging masculinities, and marginalizing feminine features.

It then selected two case studies of international law-making in the field of cyberwarfare to assess them under the established theoretical framework. The case

studies reflect an ongoing debate about the most appropriate process to develop IHL in light of a political deadlock over the negotiation of a treaty specifically designed to regulate cyber operations. The first case study encompasses the institutional processes created under the UN structure, where progress in addressing the application of IHL has been slow and fraught with political discord. Albeit slow, the process indicates that increased transparency and inclusion in the composition of the working groups have ushered in more attention to the gendered aspects of cyber conflict. Conversely, the second case study portrays a remarkable exercise in informal international law-making by legal scholars and practitioners. Nevertheless, the authority of this group is undermined not only for concentrating the worldviews of a few Western countries – however they may disagree on technical issues – but mainly for its utter disregard of gender or any other possible social factors, paving the way for a crystallization of the masculinities already enshrined in the law.

In light of the scantiness of feminist perspectives to cyber IHL both in scholarship and in practice, the research then moves to search for possible points of intersection between the feminist theoretical framework and the peculiarities of cyberspace. It explores why and how the inclusion of gender as a category of analysis can contribute to a development of IHL that does not perpetuate the unfair gender dynamics previously identified, deconstructing myths of a moral superiority of cyberweapons and raising questions about the dehumanization of war.

The discussions raised in this article only begin to scratch the surface of the interplay between gender and IHL in cyberspace. It invites further research in every possible area, from a targeted scrutiny of the gendered effects of applying long-established principles of IHL to cyberwarfare to a look at the possible gendered aspects of cyber operations in non-international armed conflicts. Virtually every feature of IHL needs a feminist review in this novel cyber environment.

The path to gendering cyberwarfare and regulation thereof necessarily goes through the deconstruction of long-held masculinist assumptions about war. If the status quo is maintained, the heavily militarized and masculinized field of security will eventually be transposed to cyberspace. As a theoretical approach that seeks the emancipation of groups generally subjugated by gender hierarchies, feminist scholars can help steer these discussions towards a more equitable path. As Cynthia Enloe wrote in a seminal book on feminism and IR (2000, 17), "the world is something that has been made; therefore, it can be remade."

References

Arvidsson, Matilda. 2018. "Targeting, Gender, and International Posthumanitarian Law and Practice: Framing the Question of the Human in International Humanitarian Law." *Australian Feminist Law Journal* 44 (1): 9-28. https://doi.org/10.1080/13200968.2018.1465331

Biggio, Giacomo. 2017. "Cyber Operations and the Humanization of International Humanitarian Law: Problems and Prospects." *Canadian Journal of Law and Technology* 15(1): 41-53. https://digitalcommons.schulichlaw.dal.ca/cjlt/vol15/iss1/4/

Beauvoir, Simone de. 2000. *Le Deuxième Sexe I, Les faits et les mythes*. Paris: Gallimard.

CCDCOE. 2023a. "CCDCOE to Host the Tallinn Manual 3.0 Process." The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/.

CCDCOE. 2023b. "The CCDCOE Invites Experts to Contribute to the Tallinn Manual 3.0." The NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/news/2021/the-ccdcoe-invites-experts-to-contribute-to-the-tallinn-manual-3-0/.

Carvalho Teixeira, Tatiana. 2023. "Gendering Cyberwarfare: Towards a Feminist Approach to the Development of International Humanitarian Law Applicable to Cyber Operations." Master's dissertation, King's College London.

Crowther, Glenn Alexander. 2017. "The Cyber Domain." *The Cyber Defense Review* 2 (3): 63-78. http://www.jstor.org/stable/26267386.

Charlesworth, Hilary, Christine Chinkin & Shelley Wright. 1991. "Feminist Approaches to International Law." *The American Journal of International Law* 84 (4): 613-645. https://doi.org/10.2307/2203269

Connell, R. W. 2005. *Masculinities*. Cambridge: Polity.

Delerue, François & Fan Yang. 2023. *Navigating Sino-European Approaches to the Application of International Law in Cyberspace*. Geneva: Geneva Centre for Security Policy. https://dam.gcsp.ch/files/doc/navigating-sino-european-approaches-to-the-application-of-international-law-in-cyberspace

Devidal, Pierrick. 2023. "'Back to Basics' with a Digital Twist: Humanitarian Principles and Dilemmas in the Digital Age." *Humanitarian Law and Policy* (blog). https://blogs.icrc.org/law-and-policy/2023/02/02/back-to-basics-digital-twist-humanitarian-principles/

Diamond, Eitan. 2014. "Applying International Humanitarian Law to Cyber Warfare". *Law and National Security: Selected Issues* 67 (138): 67-84. https://ssrn.com/abstract=3093068

Droege, Cordula. 2012. "Get Off my Cloud: Cyber Warfare, International Humanitarian Law, and the Protection of Civilians." *International Review of the Red Cross* 94 (886): 533-578. https://doi.org/10.1017/S1816383113000246

Dunlap, Charlie. 2021. "International Law and Cyber-ops: Q&A with Mike Schmitt about the Status of Tallinn 3.0." *Lawfire*. https://sites.duke.edu/lawfire/2021/10/03/international-law-and-cyber-ops-q-a-with-mike-schmitt-about-the-status-of-tallinn-3-0/

Durham, Helen & Katie O'Byrne. 2010. "The Dialogue of Difference: Gender Perspectives on International Humanitarian Law." *International Review of the Red Cross* 92 (877): 31-52. https://doi.org/10.1017/S1816383110000032.

Eichensehr, Kristen. 2014. "Review of The Tallinn Manual on the International Law Applicable to Cyber Warfare." *American Journal of International Law* 108 (3): 585-589. https://escholarship.org/uc/item/8fw1918s

Enloe, Cynthia. 2000. *Bananas, Beaches and Bases: Making Feminist Sense of International Politics*. London: University of California Press.

Farrés Jiménez, Andrea. "Gendering the Legal Review of New Means and Methods of Warfare" *Just Security*. https://www.justsecurity.org/82745/gendering-the-legal-review-of-new-means-and-methods-of-warfare/.

Fleck, Dieter. 2013. "Searching for International Rules Applicable to Cyber Warfare – A Critical First Assessment of the New Tallinn Manual." *Journal of Conflict & Security Law* 18 (2): 331-351. https://doi.org/10.1093/jcsl/krt011.

Gardam, Judith. 1988-1989. "A Feminist Analysis of Certain Aspects of International Humanitarian Law." *Australian Year Book of International Law* 12:

265-278. http://classic.austlii.edu.au/au/journals/AUYrBkIntLaw/1989/12.pdf

Gardam, Judith. 1997. "Women and the Law of Armed Conflict: Why the Silence?" *The International and Comparative Law Quarterly* 46 (1): 55-80. https://www.jstor.org/stable/760514

Grotius, Hugo. 1625. "Moderation with Respect to the Right of Killing in a Lawful War." In *The Law of War and Peace*. Re-published by Batoche Books Kitchener, 2001, Ontario, Canada.

Hansel, Mischa. 2023. "Great Power Narratives on the Challenges of Cyber Norm Building." *Policy Design and Practice* 6 (2): 182-197. https://doi.org/10.1080/25741292.2023.2175995.

Schmitt, Michael N. 2015. "Michael N. Schmitt: PILAC Lecture on Cyber Operations and IHL: Fault Lines and Vectors." *HLS Program on International Law and Armed Conflict* 56:24. https://youtu.be/ZWwrVAMSOT4.

ICRC. 2020. "International Humanitarian Law and Cyber Operations during Armed Conflicts" Position Paper, *International Review of the Red Cross* 102 (913): 481-492.

Janssens, Pauline Charlotte & Jan Wouters. 2022. "Informal International Law-Making: A Way around the Deadlock of International Humanitarian Law?" *International Review of the Red Cross* 104 (920–921): 2111-2130. https:// doi.org/10.1017/S1816383122000467.

Kello, Lucas. 2017. *The Virtual Weapon and International Order*. New Haven: Yale University Press.

Kinsella, Helen M. 2019. "Feminism." *The Globalization of World Politics* 8: 145-159. https://doi.org/10.1093/hepl/9780198825548.003.0009

Kinsella, Helen M. 2004. *Securing the Civilian: Sex and Gender in the Laws of War*. Boston: Boston Consortium on Gender, Security and Human Rights.

Lin, Herbert. 2012. "Cyber Conflict and International Humanitarian Law." *International Review of the Red Cross* 94 (886): 515-531. https://doi.org/10.1017/S1816383112000811

Lucas, George. 2016. *Ethics and Cyber Warfare: the Quest for Responsible Security in the Age of Digital Warfare*. Oxford: OUP.

Mačák, Kubo. 2021. "Unblurring the Lines: Military Cyber Operations and International Law." *Journal of Cyber Policy* 6 (3): 411-428. https://doi.org/10.1080/23738871.2021.2014919

Moynihan, Harriet. 2021. "The Vital Role of International Law in the Framework for Responsible State Behavior in Cyberspace." *Journal of Cyber Policy* 6 (3): 394-410. https://doi.org/10.1080/23738871.2020.1832550

Owens, Patricia, and Katharina Rietzler, eds. 2021. *Women's International Thought: A New History*. New York: Cambridge University Press.

Pytlak, Allison. 2020. "In Search of Human Rights in Multilateral Cybersecurity Dialogues." *Routledge Handbook of International Cybersecurity* 1: 65-78. https://doi.org/10.4324/9781351038904-7

Richardson, Diane. 2008. "Conceptualizing Gender." *Introducing Gender and Women's Studies*: 8-23. https://xyonline.net/sites/xyonline.net/files/2021-11/Richardson%2C%20Introducing%20Gender%20and%20Women%27s%20Studies%20%282020%29.pdf

Rowe, Neil C. 2015. "Distinctive ethical challenges of cyberweapons." *Research Handbook on International Law and Cyberspace*: 307-325. https://www.elgaronline.com/view/9781782547389.00026.xml

Sassòli, Marco. 2019. *International Humanitarian Law: Rules, Controversies, and Solutions to Problems Arising in Warfare*. Cheltenham: Edward Elgar.

Sharland, Lisa et. al. 2021. *System Update: Towards a Women, Peace and Cybersecurity Agenda*. UNIDIR: Geneva. https://unidir.org/publication/system-update-towards-women-peace-and-cybersecurity-agenda

Schmitt, Michael N. 2021. "Cybersecurity and International Law". *The Oxford Handbook of International Law of Global Security*.

https://doi.org/10.1093/law/9780198827276.001.0001

Schmitt, Michael N. 2017. *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge: Cambridge University Press.

Schmitt, Michael N. 2021. "The Sixth United Nations GGE and International Law in Cyberspace." *Just Security*. https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

Shereshevsky, Yahli. 2022. "International Humanitarian Law-Making and New Military

Technologies." *International Review of the Red Cross* 104, no. 920–921: 2131-2152. https://doi.org/10.1017/S1816383122000443

Stern, Orly Maya. 2019. *Gender, Conflict and International Humanitarian Law: A Critique of the 'Principle of Distinction'*. New York: Routledge.

Tanodomdej, Papawadee. 2019. "The Tallinn Manuals and the Making of the International Law on Cyber Operations." *Masaryk University Journal of Law and Technology* 13, n. 1: 67-85. https://doi.org/10.5817/MUJLT2019-1-4.

Tickner, J. Ann. 1992. *Gender in International Relations: Feminist Perspectives on Achieving Global Security*. New York: Columbia University Press.

UNIDIR. "Fact sheet - Gender in Cyber Diplomacy" https://unidir.org/publication/fact-sheet-gender-cyber-diplomacy.

United Nations General Assembly. 2021. "Open-ended Working Group on Developments in the field of Information and Telecommunications in the Context of International Security." *Final Substantive Report* 290(2). https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

United Nations Secretary General. 2005. "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." *United Nations Digital Library* A 60(202).

United Nations General Assembly. 2021. "Open-ended Working Group on Developments in the Field of ICTs in the Context of International Security: Chair's Summary." *Conference Room Paper* 290(3). https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

United Nations General Assembly. 2021. "Report of the Group of Governmental Experts on Advancing Responsible State Behavior in Cyberspace in the Context of International Security." *United Nations Digital Library* A 76(135).

United Nations General Assembly. 2013. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." *United Nations Digital Library* A 68(98).

United Nations General Assembly. 2015. "Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security." *United Nations Digital Library* A 70(174). https://digitallibrary.un.org/record/799853

United Nations. 2020. *Remarks to the General Assembly on the Secretary-General's Priorities for 2020.*

van Ingen, Michiel. 2016. "Conflict Studies and Causality: Critical Realism and the Nomothetic/Idiographic Divide in the Study of Civil War." *Civil Wars* 18(4): 387-416. https://doi.org/10.1080/13698249.2017.1297049

War Studies KCL. 2022. "Application of International Humanitarian Law on Israeli's Cyber Strategies against the Palestinians." *YouTube video*, 58:75. https://youtu.be/DT-BzeB0Tu0.

Como citar: Carvalho Teixeira, Tatiana. 2023. "Gênero na Guerra Cibernética: Rumo a uma Abordagem Feminista para o Desenvolvimento do Direito Internacional Humanitário Aplicável às Operações Cibernéticas". *CEBRI-Revista* Ano 2, Número 7: 58-80.

To cite this work: Carvalho Teixeira, Tatiana. 2023. "Gendering Cyberwarfare: Towards a Feminist Approach to the Development of International Humanitarian Law Applicable to Cyber Operations." *CEBRI-Journal* Year 2, No. 7: 58-80.

DOI: https://doi.org/10.54827/issn2764-7897.cebri2023.07.03.03.58-80.en

Recebido: 21 de agosto de 2023
Aceito para publicação: 11 de setembro de 2023