CFFP Policy Brief

Feminist Perspectives on the Militarisation of Cyberspace

CFFP
The Centre for Feminist Foreign Policy
# Table of Contents

1. Introduction .................................................................................................................. 3

2. Why cybersecurity is a feminist (foreign policy) issue ............................................... 5  
   2.1 (Cyber) Security for whom? Defining and dismantling militarisation  
       and realist security paradigms in cyberspace ......................................................... 5  
   2.2 Reframing cybersecurity in line with a feminist security understanding ............... 6

3. No security for all: About the consequences of a state-centric  
   approach to cybersecurity, and the intersecting harmful impacts of cyber  
   operations on civil society, marginalized groups and human rights advocates .......... 8  
   3.1 Feminist perspectives on cyber operations against critical infrastructure .......... 8  
   3.2 Feminist perspectives on (gendered) disinformation and online harassment ....... 12  
   3.3 Feminist perspectives on data privacy and surveillance ........................................ 15

4. What to do? Steps towards a true feminist cyber peace —  
   policy recommendations ............................................................................................... 17  
   4.1 Policy Recommendations ....................................................................................... 17  
   4.2 A note on advocacy for feminist cyber peace ....................................................... 22  
   4.3 A note on the role of the private sector ................................................................. 22

5. Conclusion ..................................................................................................................... 23

6. References .................................................................................................................... 24

7. Imprint .......................................................................................................................... 33
1. Introduction

Land, sea, air, space and - now - cyberspace? With the Russian war in Ukraine, an increasing number of cyber operations against countries of the European Union¹, and President Putin’s use of hybrid warfare,² concerns regarding an increasingly ‘insecure’ and ‘hostile’ cyberspace and its recognition as the fifth operational domain of war have been greatly intensified. Such concerns have placed the issue of cybersecurity at the forefront of national security agendas and policy debates around the world. President Biden, for example, described cybersecurity as “the core national security challenge” (Volz and Uberti, 2021).

Indeed, Ukraine’s cybersecurity authority talks about a “war in the digital realm, as well as on the ground” (Tidy, 2022), and the so-called ‘Vulkan-files’ leak in March 2023³ leaves no doubt that the Russian government and its military, and intelligence services have been cooperating with private firms like NTC Vulkan to develop offensive cyber capabilities and to plan malicious cyber operations across the globe for years (Bartz et al., 2023; Harding et al., 2023). According to the leaked documents, the intrusive and destructive tools built by NTC Vulkan do not only serve domestic purposes, such as Internet control, surveillance, and the spread of disinformation but also include training software for soldiers on cyber operations against critical infrastructure outside of Russia’s borders (ibid.). Putin’s efforts to digitally isolate Russian society are in line with those in various other autocratic regimes such as China or Iran (Association for Progressive Communications, 2022; Economy, 2018), where the Internet is strictly controlled, criticism and foreign content are censored, and the idea of a free, open, and democracy-promoting internet has become a distant vision (Satariano and Hopkins, 2022). These alarming developments are part of a broader increase in offensive cyber capabilities globally. For example, the Cyber Arms Watch transparency index⁴ shows that 60 states have developed offensive cyber capabilities (The Hague Centre for Strategic Studies, n.d.).

Feminist activists and organisations are increasingly worried about arms race dynamics in the international cyber domain and a framing of (inter-) national debates where an ‘anarchic’, ‘hostile’ cyberspace predominantly threatens national security, i.e., state boundaries, state institutions and/or regime survival. This state-centric understanding of cybersecurity is often automatically militarised (Roff, 2016: 4) and suggests that national security must be protected by building a state’s offensive cyber capabilities.

This approach favours particular policies and resource allocations that are ill-suited to address the plurality of vulnerabilities that citizens, particularly marginalized communities, face in and through cyberspace — in peacetime and in conflict. This includes online gender-based violence against women and LGBTQIA+ individuals, which has worryingly increased during the Covid-19 pandemic (The Economist, 2020; UN Women, 2020). ‘Doxing’ or the release of the private information of (women or LGBTQIA+) human rights defenders, as well as the spread of disinformation (for example, about initiatives that aim to advance human rights for all, like the Istanbul Convention), have far-reaching impacts on individuals in the digital as well as the physical world and contribute to the erosion of democratic structures, media freedom, and political participation (see CFFP, 2021a, b).⁵ Besides, a militarised, state-centric definition of cyberspace overlooks the fact that the states often undermine the (general sense of) security of their citizens and violate their own populations’ human rights. Both democratic as well as authoritarian regimes have been increasingly engaging in more or less covert, large-scale data gathering, tracking of, spying on, and surveilling their citizens (UN Human Rights Council, 2022c), which, in particular, puts human rights defenders and journalists at risk. However, the aims, methods, and consequences of surveillance within the two regimes vary greatly (see also p. 15).

¹ According to a report by Thales, the share of cyber-attacks against EU countries has increased from 9.8% to 46.5%. Moreover, the report finds that 61% of the attacks recorded globally have been of Russian origin (Thales, 2023; Vincent and Pietralunga, 2023).
² Hybrid warfare is defined as “an action conducted by state or non-state actors, whose goal is to undermine or harm a target by influencing its decision-making at the local, regional, state or institutional level” (European Center of Excellence for Countering Hybrid Threats (Hybrid CoE), 2023). Hybrid action further means combining overt and covert conventional and unconventional means, such as “disinformation and interference in political debate or elections, critical infrastructure disturbances or attacks, cyber operations, different forms of criminal activities […] [in order for hybrid actors to] veil their action in vagueness and ambiguity, complicating attribution and response” (ibid.).
³ The “Vulkan Files” are thousands of internal, secret documents and data of the Russian software company NTC Vulkan that were leaked shortly after the beginning of the Russian war of aggression against Ukraine and have ever since been analysed and evaluated by an international journalistic research team (Bartz et al., 2023). The documents entail technical details about offensive programmes and systems that are being developed for the Russian intelligence services and military (such as the hacking software ‘Skan-W’, or the system ‘Amesit’ used to control and censor the Internet in Russia, on the Crimea, and beyond) as well as information about Russia’s political long-term goals (ibid.)
⁴ The Cyber Arms Watch transparency index provides an overview and comparison of the self-declared offensive cyber capabilities (determined through publicly disclosed information) and the perceived offensive cyber capabilities (determined through the observation of outsiders and open-source information) and determines an overall “Cyber Transparency Index” for states (The Hague Centre for Strategic Studies, n.d.).
⁵ For a detailed analysis of the role of anti-gender actors and their use of disinformation campaigns, see the 2021 CFFP study “Power over Rights — Understanding and Countering the Transnational Anti-Gender Movement” (Volume I and II), available here: https://centreforfeministforeignpolicy.org/2022/11/15/power-over-rights-understanding-and-countering-the-anti-gender-campaigns/.
It is high time to broaden and advance the international debate on privacy and other human rights in cyberspace and to advance robust norms of responsible state behaviour grounded in international humanitarian and human rights law, fundamental freedoms, democratic values, and intersectional feminist perspectives. This policy brief aims to do precisely this by:

- Outlining the dangers of a militarised understanding of cyberspace and defining cybersecurity from a feminist perspective (Chapter 2)
- Analysing and highlighting the consequences of a militarised state-centric approach to cybersecurity, and the intersecting harmful impacts on civil society and marginalized groups in particular (Chapter 3), by providing examples of cyber operations against critical infrastructure, disinformation, and surveillance activities
- Developing respective policy recommendations that can inform steps towards feminist cyber peace (Chapter 4).

The policy brief builds upon a year-long project, which the Centre for Feminist Foreign Policy, financially supported by Microsoft, implemented throughout 2022 and 2023. It draws on an extensive body of research by feminist civil society and scholars and on consultations with an expert working group specifically constituted for this project. The working group included:

- Kamila Amdouni (Public Policy Advisor, CyberPeace Institute)
- Anne-Marie Buzatu (Executive Director, ICT4Peace Foundation)
- Dr Jennifer Cassidy (Diplomatic Scholar and Lecturer, University of Oxford)
- Lucas Kello (Associate Professor of International Relations, University of Oxford)
- Allison Pytlak (Programme Lead of the Cyber Programme, The Stimson Center; formerly Women's International League for Peace and Freedom).

The findings of this briefing were further informed by three closed-door multistakeholder (policymakers, scholars, representatives of civil society and the private sector) roundtable discussions from January to March 2023 on the topics of cyber operations against critical infrastructure, disinformation, and surveillance (see Chapter 3), and by an additional workshop at the European Cyber Agora⁶ in April 2023. Given its multistakeholder approach and thematic scope, this policy briefing will be relevant not only for policymakers, civil society actors, and academics working on gender (and other identity markers such as race, ethnicity, social class, etc.) and cybersecurity on the international level, e.g., in the framework of the United Nations (UN) or European Union (EU), but also for members of national parliaments, militaries, and intelligence services, or actors in the private Information and Communications Technology (ICT) sector.

Explainer: A feminist approach to security

Feminist researchers and activists conceptualise security as a transformative and people-centred approach, broadening the concept of human security. Like human security, feminist approaches to security prioritise the advancement of rights, the protection of the environment and ecosystems, access to food and health services, and economic and cultural justice. Although the latter concept “prioritises the needs and aspirations of people over states (United Nations, 2021), it fails to address gender inequality and other forms of discriminatory power relations (such as racism or colonialism) — because it uncritically accepts a universal understanding of the term ‘human’. By contrast, a feminist understanding of security makes visible the multiple and intersecting identities that are often overlooked, marginalized and/or intentionally erased in security analysis” (Hudson, 2005). This approach provides a comprehensive analysis of the complex and interdependent root causes of conflict and their gendered effects. It does so by amplifying the voices of civil society, peace advocates, movements, and marginalized communities to ensure just access to a fair distribution of resources and rights (WILPF, 2021). Consequently, a feminist understanding of security seeks to eradicate all forms of oppressive structures (including militarised foreign policy), rejects nuclear and conventional deterrence, and promotes inclusive decision-making processes at the national and international level.

This explainer is part of the glossary of CFFP’s publication: Make Foreign Policy Feminist: A Feminist Foreign Policy Manifesto for Germany (CFFP, 2021c: 11).

---

⁶ The European Cyber Agora is a multistakeholder platform, organised by Microsoft, EU Cyber Direct, and the German Marshall Fund, that aims to bring together representatives of the European Union (EU) institutions, national governments, the private sector, academia, and civil society to advance the EU’s cybersecurity policy strategy and enhance international discussions around pressing cyber issues. CFFP held a workshop titled “Feminist Perspectives on the Militarisation of Cyberspace” together with the following speakers: Allison Pytlak (The Stimson Center), Kristina Wilfore (#ShePersisted), Mikaela Rönnerman (Chair of the Horizontal Working Party for Cyber Issues of the European Council), and Dr Regine Grienberger (German Cyber Ambassador).

For more details see: European Cyber Agora 2023.
2. Why cybersecurity is a feminist (foreign policy) issue

2.1 (Cyber) Security for whom? Defining and dismantling militarisation and realist security paradigms in cyberspace

Looking at cybersecurity policies and discourses through an intersectional feminist lens means asking: Security for whom, from what, and by what means? (cf. Brown and Esterhuysen, 2019). It further means challenging dominant narratives and assumptions about (cyber-)security and the associated gendered inequalities, perceptions, and norms and highlighting their shortcomings in terms of protecting and advancing human rights and feminist security for all (in particular for marginalized communities, including women, LGBTQIA+ individuals, and racialised communities, see explainer). An intersectional feminist perspective on cyberspace also includes efforts to define and develop pathways towards cyber peace (for a detailed analysis of different understandings and concepts of and (best) practices towards positive cyber peace, see Ankersen et al., 2022).

In the dominant international discourse, cybersecurity is linked to the state — and militarised

In the international discourse, cyberspace is predominantly seen as an ‘insecure’ and ‘hostile’ environment for states. As the UN High Representative for Disarmament Affairs stated during the Security Council’s first-ever open debate on maintaining peace and security in cyberspace in 2021, “[t]he explosive growth of digital technologies around the world is opening new potential domains for conflict and the ability of both State and non-State actors to carry out attacks across international borders” (United Nations, 2021). With this statement, Izumi Nakamitsu highlighted the widespread perception that modern (increasingly digital) societies are exposed to an ever-growing threat landscape and that potential vulnerabilities will be exploited by ‘malicious’ actors. In line with this understanding, many countries have been formally integrating cyber into the military sphere⁷, releasing or updating national (cyber) security strategies, and building up their defensive and offensive cyber capabilities — therefore making cyber threats “a local point of the current national security debate” (Dunn Cavelty, 2012: 2). As early as 2010, the United Kingdom, for example, defined risks emanating from cyberspace as a “tier one” threat to national security (UK Strategic Defence and Security Review: 47), while US President Biden has made cybersecurity a “top priority” at all levels of his Administration (US Department of Homeland Security, 2022). In Russia, cybersecurity is an integral part of the broader national so-called “information security” concept, which “is governed and regulated by the state [and] to a big extent in the interests of the state” (Chislova and Sokolova, 2021: 245f). Cybersecurity is thus implicitly and/or explicitly linked primarily to the state and translates into the reduction or elimination of national vulnerabilities by “protecting oneself, building up defences, mitigating risk, deterring attacks” (Roff, 2016: 2), and strengthening national offensive cyber capabilities, often in a top-down manner. This also includes the use of cyber mercenaries, allowing states to “obscure their involvement in malicious cyber operations, seeking to gain strategic military influence by evading their responsibilities under international law” (UN Working Group on the use of mercenaries Report, 2021: 19). This state-centric understanding of cybersecurity is rooted in militarisation,⁸ which can be defined as the gradual cultural, symbolic, and material preparation for armed conflict (Enloe, 2000). If a state militarises its foreign policy, it invests in military strength and capability and discursively constructs “enemies” and “threats” in its foreign and security policy discourse (ibid.). Generally speaking, militarisation is grounded in the idea that the use of force is an appropriate option to pursue state interests (Naidu, 1985: 1). In the case of cyber, militarisation also encompasses a wider phenomenon (than the use of force), i.e., that cyber capabilities are expanded to the military with cyberspace being recognised as the fifth operational domain of warfare. A “militarisation of cyberspace” further means that “military capability is the most meaningful and effective instrument for achieving any or all national goals, and that soldiers, weapons, and wars are the most necessary and noble tools for national protection and advancement” (Enloe, 2000: 3). A recent example of this understanding is the Pentagon’s largest research, development, test and evaluation (RDT&E) budget request to date, totalling $145 billion. The budget included $13.5 billion for cyber-space activities, which, according to a Joint Staff’s director, shall be used to “defend the DoD [Department of Defence] information network, defend the nation and prepare to fight and win the nation’s wars” (Gill, 2023).

Militarised state-centric cybersecurity is rooted in gendered (neo-)realist security paradigms

A state-centric, militarised understanding of cybersecurity is based on traditional security paradigms derived from (Neo-)Realism, which assume that because of the supposedly anarchic and hostile nature of the international environment — including cyberspace — states only prosper and survive if they strive for autonomy, dominance, military power, and (military) technology (cf. Waltz, 1959, 2002). For example, the United States’ military announced in 2012 that “[d]isrupting the enemy will require the full inclusion of space and cyberspace operations into the traditional air-land-sea battle space” (cited in Hopkins, 2012).

This section draws from the CFFP Policy Briefing (2021) “How militarised is Germany’s Foreign Policy?” (Chapter 2).
Security is seen as national (state) security, taking precedence over human or feminist security (see Aggestam et al., 2019; Tickner, 1993), and can only be defended militarily. As a large body of feminist scholarship has shown, the realist security paradigm is deeply gendered. It is legitimised by identities, behaviour and values that are perceived as inherently masculine (and are thus valued more) – such as dominance, power, independence, and the willingness and ability to use weapons or even kill (see Acheson, 2019; Enloe, 1989: 199). It deprioritises characteristics considered feminine (and thus valued less) - such as cooperation, emotion, and empathy (see Connell, 1987; Peterson, 1992; Young, 1990).

As Chapter 3 will show in detail, this understanding harms “everyone and everything” (Acheson and Rees, 2020: 44), especially those whose security needs are excluded and overlooked, such as women, trans and queer-identified persons, ethnic minorities, and other marginalized groups. This is because a militarised, state-centric understanding of cyberspace favours particular policy models, behaviours, and resource allocation, ill-suited to address the plurality of vulnerabilities citizens face in and through cyberspace.

Furthermore, the dominant (cyber-)security paradigm also devalues disarmament and demilitarisation initiatives, as they are considered feminine and thus naïve, irrational, and unrealistic. This is why governments are often reluctant to commit to cooperation in and disarmament of cyberspace and to reduce (cyber) defence spending. Instead, militarised cybersecurity is predominantly thought of as a zero-sum game in ‘hostile’ cyberspace, in which one state’s attempt to gain more cybersecurity becomes an overall loss in security for the other states, which is why “one is caught in a vicious cycle of defense, development, exploit, defense, development, exploit” (Roff, 2016: 7).

Consequently, resources are continuously diverted from endeavours that would make people more secure, like investments in mitigating the climate crisis or in infrastructure that is critical for marginalized communities such as women’s shelters (see Chapter 3.1), the pursuit of gender equality, social justice, and human rights in all offline and online spaces.

The militarisation of cyberspace replicates patriarchal power structures and systems of oppression

The militarisation of cyberspace is thus “an expansion of the patriarchal structures of power that perpetuate violence and repression. This not only overlooks systemic and root causes of violence but sets out to exacerbate and create violence in a new medium where it does not necessarily otherwise occur” (Pytlak, 2021). Also, a militarised state-centric approach to cyberspace and cybersecurity feeds into the (too) narrow definition of cyber peace as ‘negative’ cyber peace, i.e., the absence of hostile or malicious activity in cyberspace (Roff, 2016: 2).

A growing community of feminists and feminist civil society organisations, policymakers, scholars and private companies have challenged this reduced notion of cybersecurity and ‘negative’ cyber peace and have been dedicated to defining and operationalising a ‘positive cyber peace’.

2.2 Reframing cybersecurity in line with a feminist security understanding

A feminist approach to the cyber landscape assumes that cyber(-space) is what states and the actors within states make of it (Roff, 2016: 7), rejecting the dominant realist assumption that cyberspace is an ‘insecure’ and ‘hostile’ environment from the start. States and non-state actors, through their interactions, values, norms, and identities, can construct the international digital space in alternative ways, which will then also influence their respective (re-)actions in or through cyberspace (ibid.). This is not to say that a feminist approach would ignore or even neglect the ever-evolving cyber threats and malicious actors that states and (digital) societies face, but that it is convinced of the possibility of creating a peaceful cyberspace. This fundamental conviction changes and expands the options for political action – away from spirals of militarisation and the build-up of national cyber arsenals towards cooperative approaches in favour of those who should benefit from cyberspace: people and societies across the globe.

“Feminist perspective is critical of and rejects a wholly state-centric understanding of cybersecurity. It is a call to put people first.”

Allison Pytlak, The Stimson Center, formerly WILPF

---

9 For example, Microsoft called for a “Digital Geneva Convention”, focusing on human cybersecurity and committing governments to protect civilians from nation-state attacks in times of peace (Kurbalija, 2017). Moreover, academia has been taking a more nuanced perspective to categorise cyber activities on a larger spectrum between peace and war. Lucas Kello (2021), for example, uses the term “unpeace” – defining a mid-spectrum conflict that is neither physically destructive like war, but too damaging socially and politically to be considered peacetime activity.

10 This understanding stems from International Relations scholar Alexander Wendt who, in his famous article “Anarchy is What States Make of It: The Social Construction of Power Politics” (see Wendt, 1992), made clear that anarchy and the egoistic striving for dominance, (military) power and preparation for conflict that theories like (Neo-)Realism derive from this, is not inherent in the international system, but a socially constructed concept.
Accordingly, a feminist understanding of cyberspace recognises its inherent civilian nature, where internet users around the world interact, communicate, and access information. A feminist approach to cyber thus builds upon existing human-centric and human-rights-focused approaches to cyberspace, which place the individual (not the state) as the primary referent of security. Again, it does not contest that cyber threats against nation-states exist and can put national (state) security at risk but focuses on the humanitarian impacts of activities in and through cyberspace on marginalized communities and the consequences of a much too narrow state-centric approach.

Nearly ten years before, the UN Human Rights Council affirmed that “the same rights that people have offline must also be protected online” in its landmark resolution on the promotion, protection and enjoyment of human rights on the Internet (Human Rights Council, 2012). And the Geneva Declaration, adopted at the International Telecommunication Union’s (ITU) World Summit on the Information Society in 2003, already underlined several features of a human-centric approach to cyberspace. The signatory states expressed their “commitment to build a people-centred, inclusive and development-oriented Information Society, where everyone can create, access, utilize and share information and knowledge, enabling individuals, communities and peoples to achieve their full potential in promoting their sustainable development and improving their quality of life, premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights” (Geneva Declaration of 2003: A.1., see International Telecommunication Union, 2003). They also highlighted the importance of “paying particular attention to the special needs of marginalized and vulnerable groups of society” when building digital societies (ibid.: A.12., A.13.). Consequently, as Katrin Nyman Metcalf puts it with reference to the Estonian Cybersecurity Strategy (2019-2022), “cybersecurity does not mean protecting technological solutions; it means protecting digital society and the way of life as a whole” (Republic of Estonia, 2019).

To date, however, there is no universally agreed-upon definition of cybersecurity, making it “easier for some governments to violate basic rights in the name of a broad ‘cybersecurity threat’” (Rossini and Green, 2015: 10). To counter this development, the Internet Free and Secure Initiative (IFSI) developed a definition that is instructive for a feminist understanding of cybersecurity, as it centres the individual, i.e., human security: “Cybersecurity is the preservation — through policy, technology, and education — of the availability, confidentiality, and integrity of information¹³ and its underlying infrastructure to enhance the security of persons both online and offline” (IFSI n.d.).¹⁴ This also means that human rights and fundamental freedoms must be at the core of cyber policy development and decision-making. As we have shown above, however, the dominant international discourse, existing cyber laws and strategies, and other governmental activities aiming to increase cybersecurity often leave human rights aside, “or worse, view human rights as an impediment to cybersecurity […] and itself become the source of insecurity” (Brown and Esterhuysen, 2019). With the adoption of a resolution on the Programme of Action (PoA) on cybersecurity that is supposed to be established¹⁵ after the UN Open-ended working (OEWG) group 2021-2025 on Developments in the Field of Information and Telecommunications in the Context of International Security as a permanent, inclusive mechanism, a silver lining has appeared. In its preamble, the resolution underlines “the necessity of bridging digital divides, building resilience in every society and sector, and maintaining a human-centric approach” and of narrowing the “gender digital divide” and promoting women’s participation and leadership in decision-making processes related to the use of ICTs and international security (emphasis added, UN First Committee, 2022). Nevertheless, it must ensure that such human-centric perspectives will not be siloed into their own paragraph but mainstreamed throughout the institutional framework, operational activities and policies of national and international entities working on cybersecurity.

A feminist perspective on the militarisation of cyberspace goes further than these approaches that focus on human rights and women’s participation and acknowledges that not everyone’s security and human rights are evenly impacted through cyber operations. Indeed, it recognises that sexist and racist power imbalances in cyberspace are informed

¹¹ It is generally difficult to clearly distinguish civilian and military interests and actors in cyberspace, a problem that is, at least partly, rooted in the nature of cyber technology. Surveillance technologies, for example, albeit being developed for peaceful purposes, citizens’ enhanced security or the benefits of so-called ‘smart cites’, can be repurposed easily, as chapter 3.3 on surveillance shows in more detail.

¹² For an overview of the hundreds of definitions related to cybersecurity and cyberspace, see the Global Cyber Definitions Database by the Cyber Security Initiative: cyberdefinitions.newamerica.org.

¹³ This definition respects the ISO 27000 standard for information security and management systems and their requirements in order to include the work of the technical community (cf. IFSI n.d.).

¹⁴ The IFSI builds on the work of the “Internet Free and Secure” Working Group of the Freedom Online Coalition (FOC), a partnership of 36 governments committed to Internet freedom and the protection of human rights, see FOC n.d.). For more information, see: About the Internet Free & Secure Initiative - Internet Free and Secure Initiative.

¹⁵ So far, it has not yet been fully settled if and when the PoA will be established. The respective resolution on a “Programme of action to advance States’ behaviour in the use of information and communications technologies in the context of international security” adopted by the UN First Committee in 2022, calls on states “to discuss, and further develop if appropriate, this framework” (United Nations First Committee, 2022), and determines that the PoA will be discussed in the 78th session of the UN General Assembly and in the meetings of the OEWG 2021-2025 (ibid.).
by and reinforce power imbalances in our physical world and that various forms of digital harm and malicious cyber operations — like disinformation campaigns, surveillance, online gender-based violence (GBV), and attacks against critical infrastructure — intersect with misogyny and other (patriarchal) systems of oppression (such as capitalism and its clickbait business models, see p. 14) as will be shown in the next Chapter in more detail. In cyberspace, politically marginalized people are the subject of discrimination and violence, even though they do not enjoy the same rights and do not have the same opportunities and resources to access cyberspace — both in terms of cyber technologies and participation in cyberspace as well as in terms of cyberspace governance (Mhajne et al., 2021).

Moreover, a feminist approach to cyberspace recognises that it is often the state that violates human rights in and through cyberspace, thus rendering marginalized individuals and communities even more insecure. This danger is particularly present when we speak about surveillance, which in the name of detecting threats, can become a risk to citizens’ privacy and personal freedom (Candra and Wardoyo, 2020).

So, a feminist approach to cyber aims at positive cyber peace by making everyone secure through the reduction of vulnerabilities in cyberspace on all levels (national, community, and individual) and by establishing national and international legal and normative frameworks that centre the needs and perspective of those most marginalized, which are usually those most affected by existing cyber policies and malicious activities in digital spaces. Failing to address these issues through national and international cybersecurity frameworks will not only fail most of us but also seriously endanger democratic structures and our international human rights architecture, as the next Chapter will clarify.

### 3. No security for all: About the consequences of a state-centric approach to cybersecurity, and the intersecting harmful impacts of cyber operations on civil society, marginalized groups and human rights advocates

To highlight the consequences of the militarisation of cyberspace, as well as related state-centric approaches to cybersecurity, and the intersecting harmful impacts of cyber operations on civil society, marginalized groups, and human rights advocates, this briefing focuses on three examples: cyber operations against critical infrastructure (Chapter 3.1), disinformation (Chapter 3.2), and surveillance (Chapter 3.3).

#### 3.1 Feminist perspectives on cyber operations against critical infrastructure¹⁶

Cyber operations against ‘critical infrastructure’ are arguably the most striking and tangible example of the humanitarian impact of malicious cyber activities. This is because they materialise in the disruption and physical violence against the systems and processes that ensure the well-functioning of a state and the well-being of its population, thereby affecting many social classes and economic sectors. The steep increase in such operations, especially in the course of the Russian war in Ukraine, has catalysed new discussions on cyber defence and has exacerbated existing concerns about hybrid threats and the resilience of critical infrastructure, which EU Commission president Ursula von der Leyen recently called “the new frontier of warfare” (EU Commission, 2022). Not only has the total number of cyber operations against Ukraine tripled over the past year (Sabbagh, 2023), but as of May 2023, the CyberPeace Institute has counted nearly 50 countries affected by over 1,600 cyber operations relating to the Russian war in Ukraine.¹⁷ These operations have included distributed denial-of-service (DDoS) operations, deletion of data or damage to systems through malware and have impacted 23 sectors, most of which are widely defined as ‘critical infrastructure’, such as financial, public administration, and transport sectors (CyberPeace Institute 2023a).

However, cyber operations against critical infrastructure have not only been a matter of concern in conflict-affected contexts but also in times of peace. For example, the German parliament’s IT system was shut down for four days following a cyber operation in 2015 (DW, 2015), and during...
the Covid-19 pandemic, various cyber operations were directed against medical facilities and organisations working on Covid-19 vaccines (Cursino, 2021; Milanovic and Schmitt, 2020).

Forgetting about those (not) protected: gaps in dominant understandings of critical infrastructure

Even if such disruptions of critical infrastructure have usually led to outrages in the media and heightened political debates on national cybersecurity, “the link between those infrastructures and the human lives that they service and protect has not been made” (Reaching Critical Will, n.d.). For example, it is rarely discussed that cyber operations against hospitals not only lead to data breaches and disruptions of teaching and learning. Still, it can also cause a reallocation of resources away from education and towards cyber resilience, for example. Suppose the overall school budgets are not increased to compensate for this reallocation. In that case, it affects the educational rights, needs, and well-being of children—one of society’s most vulnerable groups (e.g., Klein, 2022). Seldom is it made clear by state actors that cyber operations against hospitals can mean that people are killed because equipment fails or medicine is not available quickly enough (e.g., Tidy, 2020). However, civil society and academia have been leading growing efforts to highlight the humanitarian and societal impact of cyber operations against the healthcare sector (for example, the CyberPeace Institute provides data on over 500 cyber operations across 43 countries within its “Cyber Incident Tracer #HEALTH”). Additionally, it is rarely questioned who is being protected according to the dominant understanding of critical infrastructure and who is being left behind.

A twofold feminist approach to critical infrastructure protection

Feminist perspectives on critical infrastructure provide an effective tool to fill these gaps in two respects. Firstly, a feminist approach is a means of ‘gendering’ the critical infrastructure protection status quo. It does so by highlighting the differentiated impact of cyber operations against critical infrastructure on marginalized groups and individuals based on their gender or other markers of identity. In the state-centred militarised discourse on cybersecurity, the humanitarian long-term consequences of cyber operations against critical infrastructure are hardly addressed (and the consequences of those cyber operations against infrastructures that have not yet been defined as ‘critical’ are even less so). Public authorities also fail to collect gender-disaggregated data on the human harm following these incidences. We owe it to (feminist) civil society that there have been detailed documentation of individual cases and more extensive studies providing empirical evidence. Secondly, to not reproduce the underlying patriarchal systems of oppression at play, an intersectional feminist approach reformulates and extends the dominant definition of critical infrastructure that is already gendered per se. The examples of cyber operations against the health, ICT, humanitarian, development, and civil society sectors19 will illustrate both points in the following section.

Harming those already most vulnerable: cyber operations against the Health sector

In their study ‘Why Gender Matters in Cybersecurity’, feminist scholars Allison Pytlak and Deborah Brown show that cyber operations against the health sector, such as hacking and the resulting data breaches, never take place in gender-neutral settings: “even if they are not targeting people specifically on the basis of gender, they can have a more severe impact on women and LGBTQ people because of historical and structural inequalities in power relations based on gender and sexuality” (Pytlak and Brown, 2020: 12). To illustrate this point, Pytlak and Brown used the example of a data breach in the public health system of the municipality of Sao Paulo in July 2016, and the release of information about pregnancy and abortion care that affected almost 16,000 women and people with a uterus. In addition to a violation of their privacy, as abortion is illegal in Brazil, over 4,000 of those individuals (and their doctors) who had terminated their pregnancies were subject to potential criminal charges (ibid.). Additionally, regardless of the legality of abortions, the release of such medical data, as was the case when Australia’s largest health insurer Medibank refused to pay $10 million to hackers (Mao, 2022), can discourage women and people with a uterus from exercising their reproductive rights and seeking medical care for fear of verbal gender discrimination or even physical gender-based violence (GBV), given the ongoing stigmatisation and tabooinisation of abortions in patriarchal societies. The Medibank leak brings to the fore another gendered feature of cyber operations against critical infrastructure. In this case, it showcases the capitalisation of misogyny associated with reproductive health (see CQU University Australia, 2022), a common business model facilitated in and through cyberspace at the expense of marginalized individuals and groups (see also Chapter 3.2 on disinformation).

The United States’ new National Cyber Strategy, acknowledging that “the greatest harm falls upon the vulnerable populations for whom risks to personal data can produce disproportionate harm” (United States Cybersecurity Strategy, 2023: 19), is a first step in the right direction—but it is clear that there remains an urgent need for clearer identification of vulnerable groups and their respective needs to protect them adequately.

¹⁸ The “Cyber Incident Tracer #Health” is available here: Cyber Incident Tracer #HEALTH (cyberpeaceinstitute.org).
¹⁹ This includes non-governmental entities working in the field of humanitarian aid, development cooperation, and civil society or non-governmental organisations (NGOs) advocating for human rights and fundamental freedoms in the broadest sense.
Cyber operations against the ICT sector and Internet shutdowns

Other examples illustrating the gendered harm caused by cyber operations against critical infrastructure are the mis-/abuse or complete shutdown of the Internet and digital services. For instance, trans-exclusionary radical feminists (TERFs), and in particular the TERF organisation Women’s Liberation Front, have been using Google Maps to map, track, and target children’s hospitals that provide transition-related medical care in the United States and other establishments across the globe serving trans peoples’ health and well-being (Factora, 2022). Just as in the cases mentioned above, such attempts pose serious online and offline risks to the listed infrastructures and the people behind them – consumers and providers of trans medical services and support.

Data by the #KeepItOn coalition in collaboration with the non-profit organisation Access Now shows that internet shutdowns have been increasingly weaponised across the globe and have coincided with documented human rights abuses, for example, during conflict and protest (Access Now, 2022a).²⁰ The cyber operation against the Viasat-owned satellite system KA-SAT (‘Viasat hack’), especially in the context of the Russian war against Ukraine,²¹ made clear that the Internet is a critical infrastructure and should be treated as one. It can be a lifeline in the literal sense, or as Azadeh Akbari²² writes about the internet shutdown by the Iranian regime and its impact on especially women: “disconnection kills” (Akbari, 2022). The ‘Viasat hack’ predominantly affected parts of Ukraine’s defence forces’ communication at the beginning of the Russian invasion on 24 February 2022 (Burgess, 2022) and strategic locations like Mariupol (Donetsk) and Kyiv. The cyber operation hit amid the first reports of civilian casualties and targeted areas when civilians urgently needed digital platforms and services to flee and seek shelter (NetBlocks, 2022).

The internet shutdown in Iran illustrates two points that dominant state-centric discourses on cybersecurity and critical infrastructure often neglect. Firstly, humanitarian harm does not necessarily need to be caused by foreign actors; states can decide to disrupt digital services critical to the population under their jurisdiction. The purpose of partial or complete Internet shutdowns can hinder mobilisation or information sharing and impose restricted national networks under governmental surveillance (see Chapter 3.3), limiting and violating freedom of expression, the right to privacy, and other human rights offline and online. As Akbari explains: “Activists [in Iran] have seized the possibilities that digital technologies offer in recent years, with campaigns not only for changing laws and policies but also to bring to light more taboo issues such as the policing of the female body, domestic violence, violence in the workplace, sexual harassment and the Iranian #MeToo movement. This is why the regime has moved quickly to shut down internet access, blocking social media platforms such as Instagram and WhatsApp” (2022). Secondly, the case of Iran highlights the disproportionate gendered impact of Internet shutdowns which has also been well-documented in other countries like India, Venezuela, and Pakistan in terms of women’s and other marginalized groups’ personal safety, education, professional and economic situation, and their emotional well-being (see Pytlak and Brown, 2020: 8-12).

Status quo: definitions of critical infrastructure feed into gendered state-centric security paradigms

In national cyber strategies and international discourses, critical infrastructure is generally defined as facilities or institutions that are “crucial to the functioning of society” and “public security” (German Cyber Security Strategy, 2021). Examples include supply chains, energy networks, ICT infrastructure, health and finance services, and the water and agriculture sector (e.g., US Cybersecurity and Infrastructure Security Agency, n.d.), which, if destroyed or rendered unavailable, would “significantly impact the social or economic well-being of the nation” (emphasis added, Australian Government 2015), national defence, and national security (Australia’s Cyber Security Strategy, 2020). The United Kingdom’s definition of critical infrastructure includes a notion of the risk of “significant loss of life or casualties” if essential services are targeted, and the European Union’s definition of critical infrastructure from 2008 recognises that the purpose of the protection of such infrastructures is “to contribute to the protection of people” (Council of the European Union, 2008; UK National Protective Security Authority, n.d.). However, although the EU’s new NIS 2 Directive²³ and Critical Entities Resilience (CER) Directive both define a broad range of sectors, subsectors and categories of entities of high criticality (see Annex I, NIS 2 Directive;
Annex of Directive 2022/2557\(^{24}\), they do not differentiate groups of affected citizens, just like the definitions of nation-states. This neglects the crucial gender-specific security and health-related needs, which is also true for cyber defence, mainly referring to the protection of critical infrastructure at the national level (see Menninger and Datzer, 2022). By not including the feminist security, gender-sensitive and harm-responsive perspectives, or references to the Women, Peace, and Security (WPS) Agenda (UN Security Council Resolution 1325), existing national definitions of critical infrastructure reproduce and feed into gendered (neo-)realist security paradigms that solely focus on the state and national security, thus overlooking individual (human) security and not differentiating between various (marginalized) groups and their security needs (see p. 5f).

Similar conclusions can be drawn at the international level. Although the Report of the Office of the UN High Commissioner for Human Rights on Internet shutdowns acknowledges that “[i]nternet shutdowns also undermine access for women and girls to critical support and protection, exacerbating the gender divide” (Office of the High Commissioner for Human Rights [UNHCHR], 2022), 10, existing efforts made by the state community to define critical infrastructure as part of a set of norms of responsible state behaviour in cyberspace\(^{25}\) lack a human, feminist security and gender-sensitive perspective.\(^{26}\) Moreover, the legal status of such norms that prohibit states from “conduct[ing] or knowingly support[ing] ICT activity contrary to [their] obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public” (UN Group of Governmental Experts, 2015: 8) is contradictory. Due to the lack of a universally agreed-upon definition of critical infrastructure, there is no clarity about which cyber operations are prohibited by international law (Haataja, 2022), which creates potential loopholes for malicious state and non-state actors. This reinforces the (perceived) threat of malicious operations and creates a general sense of insecurity, which is likely to lead to the further militarisation of cyberspace and excessive investments in cyber defence and resilience that go beyond the necessary level of protection. Thus, diverting resources away from other endeavours that would enhance the security of citizens.

Feminist (re-)definitions of critical infrastructure that do not leave anyone behind

A feminist approach thus makes clear that (inter-)national norms and measures intended to protect critical infrastructure must be designed with the needs of those who are disproportionately affected by and/or vulnerable to cyber operations in mind. It also requires a re-definition of critical infrastructure from a feminist perspective to provide a more nuanced and inclusive understanding of what kind of infrastructure is actually ‘critical’ for whose survival and well-being and needs enhanced protection.

For the health sector, for example, this means providing (enhanced) protection for establishments offering medical care for trans people, abortion, critical services, shelter, and/or emotional support for women and LGBTQIA+ people. Regarding ICT infrastructure, this means setting international norms that prohibit and, ideally, sanction internet shutdowns and surveillance tools that restrict access to free and open information, communication, and interaction online (see Chapter 3.3).\(^{27}\) Furthermore, civil society organisations and non-governmental humanitarian and international development organisations (NGOs) must be included in the process of establishing a feminist (re-)definition of critical infrastructure via consultations and need to be considered ‘critical’ themselves. They are integral to the functioning of democracy. They hold national and foreign governments accountable; they defend and advocate for human rights and are often the first to provide assistance in crises and conflicts. However, due to significant and chronic budget and time constraints, organisations in the humanitarian, development, and civil society sector are ill-equipped to defend themselves against potential cyber operations, making them even more vulnerable (they can be considered particularly vulnerable to cyber operations from the start, given the nature of their work, so their inability to invest in cyber resilience and sufficiently train staff only exacerbates the status quo/adds another layer of vulnerability).

Additionally, as the CyberPeace Institute finds, humanitarian NGOs, in particular, often operate in contexts “with limited or unreliable infrastruc-

---


\(^{25}\) The basis for cybersecurity norms and policies at the UN was laid by the work of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – short UN GGE – between 2004-2021. In 2020, the above-mentioned UN CENWG was established by the UN General Assembly and will continue the work on cyber issues until 2025 (see UN General Assembly, 2020).

\(^{26}\) For example, the General Assembly resolution 58/199 on the “Creation of a global culture of cybersecurity and the protection of critical information infrastructure”, cited in norm ‘g’ as part of the recommended “Norms, rules and principles for the responsible behaviour of States” in cyberspace by the UN GGE, does not even contain the word “human rights”, let alone a gender-sensitive perspective on critical infrastructure protection.

\(^{27}\) This briefing acknowledges that it is unlikely that authoritarian countries like Russia or China would (currently) agree to such norms. Nevertheless, democratic states taking a norms-based approach to cyberspace need to advocate for (norms of) responsible state behaviour in cyberspace, e.g., in international fora such as the United Nations, and support civil society working towards similar goals. Only then can we uphold the goal of a cyberspace that is free and open for all, and, in the long run, stay on the pathway towards achieving majorities for such a norms-based approach.
Feminist Perspectives on the Militarisation of Cyberspace

A feminist approach to cybersecurity highlights the humanitarian consequences and differentiated impact of cyber operations against critical infrastructure on marginalized groups and individuals based on their gender or other identity markers. It clarifies that the definition of critical infrastructure is not exhaustive and needs to include further critical entities, such as health facilities for LGBTQIA+ people, or entire sectors, such as the development and humanitarian sector. Those are essential for civil society’s (in particularly marginalized groups’) well-being, enjoyment of human rights and freedoms, (human) security, for their political participation — and/or even for their survival. Only if we make the (security) needs and lived experiences of marginalized groups the centre of the discussion around critical infrastructure protection can we reduce cyber harm and save lives.

3.2 Feminist perspectives on (gendered) disinformation and online harassment

The Internet has led to the democratisation of knowledge and information. It has provided crucial opportunities for human rights activists, women’s political participation, and civil society’s political mobilisation, particularly in autocratic regimes where offline spaces are heavily restricted, as shown above. However, digital spaces, especially social media platforms, represent a curse with misinformation, which is “the deliberate dissemination of false or inaccurate information to discredit a person or organisation” (CSI Library, n.d.). This is not to be confused with misinformation, which is “the sharing of inaccurate and misleading information in an unintentional way” (ibid.). The extent of the disinformation threat has recently been illustrated by disinformation campaigns around the coronavirus (Covid-19) that endanger public health (e.g., EU Commission, n.d.) and around the Russian war in Ukraine. In the latter case, Russia and pro-Russian actors used massive (dis)information operations to justify military action against Ukraine, undermine the country’s ability to resist, derail support for Ukrainian resistance internationally and within Russia, and shape public opinion about the war, as a recent report by the Atlantic Council shows (Atlantic Council, 2023). Even though the weaponization of disinformation is nothing new, rapidly changing ICTs, social media platforms, the increasing use of messaging apps, artificial intelligence (AI), and big data analytics have facilitated its spread and the targeting of specific user groups (OECD, 2020, 2022). Thanks to a growing body of feminist research, it is a well-established fact that disinformation disproportionately and increasingly affects and targets individuals or groups based on their gender — a phenomenon defined as “gendered disinformation” (e.g., Di Meco, 2020; Judson et al., 2020). Additionally, gendered disinformation means that gender narratives are weaponised by state or non-state actors to promote political, social or economic goals (ibid.).

“Gendered disinformation is a risk to democracy and human rights”
Kristina Wilfore, #ShePersisted

A militarised state-centric understanding of cybersecurity and its three-fold ignorance of the impact of gendered disinformation and online harassment

The dominant international, militarised, state-centric narrative around security in cyberspace is ill-suited to address and mitigate this (gendered) disinformation threat in three respects. This is because it ignores the humanitarian long-term impact of gendered disinformation and online harassment, neglects the latter’s national security dimension, and does not sufficiently acknowledge the role of the private sector, especially social media companies. By recognising that “gendered disinformation is part of the broader weaponization of the Internet” (Wilfore, 2023; see also Chapter 3.3. on surveillance), and by taking an intersectional human security and multi-stakeholder approach, a feminist perspective sheds light on these exact issues and provides pathways to mitigate them.

The humanitarian impact of gendered disinformation and online harassment

A feminist approach to disinformation addresses the (gendered) disinformation threat itself. It highlights other forms of online discrimination (e.g.,

---

28 The CyberPeace Institute has been aggregating data on such incidences and offers support for NGOs to help them prevent and recover from cyber operations in the framework of the “Humanitarian Cybersecurity Center” (CyberPeace Institute, n.d.)

29 Often discussed together with disinformation, “fake news” are defined as the “intentional falsification and fabrication of news-based information with the purpose to harm and deceive people” (CSI Library, n.d.).
on the basis of sex, religion, race, or ethnicity) and the risks that intersect with it, such as psychological gender-based violence. It acknowledges that intersecting forms of digital harm can also develop into physical violence and thus undermine the affected individual’s fundamental freedoms and human rights, such as the right to freedom of expression and political participation or the right to bodily integrity. This is why states play a crucial role in countering disinformation – a fact also highlighted by the UN Human Rights Council (2022b), albeit with a limited gender-sensitive approach. States must take appropriate measures to protect marginalized groups under their jurisdiction.

For example, Meta’s algorithms intensified online discrimination and hatred against the Rohingya Muslim community in Myanmar before the atrocities, whereby Rohingya women and girls in Rakhine State were specifically targeted (Amnesty International, 2022). In Brazil, false reports about drug trafficking in connection with the black, bisexual environmentalist and city councilwoman Marielle Franco who was known to speak up for the marginalized and criticise the police, were spread after she was murdered in 2018 (Hauch and Anderson, 2018). Even two years later, when a Black journalist and activist published an article reviewing the evidence of former Brazilian President Jair Bolsonaro’s links to the murder of Franco (that he has summarily dismissed), she was accused of spreading fake news by Bolsonaro (Santana, 2020). A 2021 UNESCO discussion paper rightly highlights that “orchestrated disinformation campaigns operationalise gendered violence to chill critical reporting” and that, at the same time, reporting on disinformation can be a trigger for heightened attacks against, e.g., women and non-binary journalists (UNESCO, 2021).

The study “Troll Patrol” by Amnesty International analysed millions of tweets received by 778 women journalists and politicians throughout 2017. It found that, on average, these women received one abusive or problematic tweet every 30 seconds, amounting to 1.1 million tweets in total. Their political orientation did not affect these findings. However, their race did: Black, Indigenous, and women of colour (BIWOC) were 34% more likely to be affected by abusive content online (Amnesty International, 2018). This underlines the importance of an intersectional feminist perspective once more.

Additionally, analyses carried out in the context of the 2020 United States federal elections and the 2021 German federal elections do not only prove that women in politics – and increasingly also their partners or children – are targeted by online hate and disinformation more often than their male counterparts, but that disinformation also has a more stringent impact on their political careers or electoral success (Di Meco, 2019; cf. #ShePersisted, 2023; Smirnova et al., 2021; Tumulty et al., 2020). Social media posts aimed at German chancellor candidate Annalena Baerbock (now Germany’s Foreign Minister), for example, often referred to her gender and used belittling language to question her competence. Other women members of the German parliament also reported having similar experiences (Klingert, 2021). As Kristina Wilfore, a development and democracy expert and co-founder of #ShePersisted, explains: “gendered disinformation campaigns build on, and are rooted in, deeply set misogynistic frameworks and gender biases that portray masculine characteristics as those fit for leadership while painting women leaders as inherently untrustworthy (insinuating a woman is dishonest or not trustable is a tried and true attack), unqualified (one of the biggest barriers women face when seeking office), un inteligent (tropes about women as dumb and unfit for the job are a prominent feature of gendered disinformation, made worse with objectifying sexualized content), and unlikeable (which, for women, can be the death knell of their campaign)” (Wilfore, 2022: 131, cited in #ShePersisted, 2023).

Consequently, gendered disinformation can not only cause serious mental or physical harm on a personal level, but it also impacts women’s and other marginalized groups’ ability and willingness to participate in (online) politics and activism, or to pursue political careers, with the risk of self-censorship (ibid.; Pavlova, 2023).

Another disturbing development related to disinformation and digital (gender-based) violence is the spread of deepfakes. Deepfakes can be defined as video or audio files that are manipulated through artificial intelligence (Hate Aid, n.d.). Algorithms in programmes or apps are used to produce fake visual or audible material: they can, e.g., swap the face of any person into a video or imitate voices and add new text, putting the targeted person into another context or foreign state to their advantage (ibid.). Consequently, there is “a growing danger that deepfakes massively deceive civil society and manipulate public opinion” (ibid., authors’ translation), for example when fake statements by political actors are used for political propaganda and disinformation which suddenly appear credible – deepfakes thus threaten democratic structures (ibid.). Women and other marginalized groups are disproportionately affected by deepfakes. With only one click, the face of any person (currently, it is mostly exclusively done with women’s faces) can be swapped into pornographic videos. In addition to the psychological harm and possible trauma resulting from pornographic or other deepfakes, it is difficult for affected individuals to prove that such videos are fake. This puts women in politics or different leadership positions at even higher risk as they face year-long struggles to restore their reputations and regain the citizens’ trust (ibid.).

The (inter-)national security dimension of gendered disinformation and online harassment

The aforementioned Russian (dis)information operations targeting Russian and foreign societies leave no doubt that disinformation has become a
matter of international and national security, undermining peace and stability. However, quite ironically, dominant state-centric discourses on cyber usually disregard the fact that gendered disinformation also has an explicit (inter-)national security dimension. As Di Meco and Wilfore (2021) argue, “[p]ushing women out of the political arena is often only the first step of a broader, dangerous strategy to erode democracy and human rights […] and this tech-enabled backlash against women’s rights has broader ramifications for global peace and security”. Indeed, gendered disinformation and ICT-facilitated gender-based violence help normalise misogynistic narratives and fuel anti-gender norms and activities, which result from them at unprecedented scales. Wilfore calls this a “behaviour modification machine” (Wilfore, 2023). Authoritarian leaders and the anti-gender movement employ gendered disinformation campaigns as a tactic to influence elections, to “unsettle citizens’ faith in democratic institutions” (Colomina et al., 2021), to hinder human rights advocacy, or to deliberately sow division and deter governments from supporting particular policy goals (as was the case in Bulgaria in 2018 when disinformation hampered the ratification of the Istanbul Convention (see CFFP, 2021a)); “The challenge, especially with disinformation campaigns […] is that it becomes challenging to break down the points they make argumentatively. Once these soundbites make it into the public discourse, they become nearly impossible to stop […]. [creating] enough noise about the issue to make policy change difficult, even for progressive governments” (ibid.: 45).

Furthermore, human rights organisations have warned of attempts by anti-gender actors to enact international cyber laws and policies. The Russia-introduced international “Convention on countering the use of information and communications technologies for criminal purposes”, for example, is largely at odds with obligations to protect human rights under the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR) (Human Rights Watch, 2022). Such vaguely worded emerging laws on cybercrime violate international standards of freedom of expression and can be (mis)applied to monitor and discredit human rights advocates instead of tackling disinformation campaigns, for example.

A note on big tech and social media companies, “effective control” and “clickbait” business models

In March 2023, recognising that disinformation undermines peace and stability, the Prime Ministers of Ukraine and seven other Central and Eastern European states addressed an open letter to major tech companies such as Meta, calling for enhanced measures to fight this threat (Reuters, 2023). However, gendered disinformation was not mentioned — nor the critical role that big tech and social media companies play in tackling it. As the study “Monetizing Misogyny” by #ShePersisted has clarified, the immense spread of gendered disinformation is not only rooted in misogyny but is instead connected to the latter’s weaponization by malicious state and non-state actors and monetisation by major digital platforms and their “clickbait” business models (#ShePersisted, 2023; see OECD, 2020). Indeed, “[harmful narratives are boosted and amplified through algorithms that make such content sticky and often viral, through recommender systems built to maximise attention, and features that facilitate its rapid and widespread distribution” (Di Meco, 2023). Social media companies often have “effective control” over the technologies facilitating the spread of gendered disinformation. Still, states remain responsible for the protection of the fundamental freedoms and human rights of the population under their jurisdiction, which is why they need to develop and improve (inter-)national legal frameworks regulating these platforms.

**Tackling (gendered) disinformation — without violating human rights at the same time**

In this regard, the European Union’s Digital Services Act moves in the right direction. It aims to create a safer digital space where there is greater democratic control, oversight and less exposure to illegal content and where the mitigation of the disinformation threat shall be ensured through, for example, increased transparency in digital platforms’ content moderation processes and outcomes, and the users’ opportunities to inform themselves about and contest content removal (EU Commission, n.d.b). Still, key questions remain regarding effective enforcement and equitable inclusion of civil society in efforts to tackle illegal content and establish due diligence obligations for online platforms (see Allen and Stockhem, 2022). Special attention must be paid to the danger that counter-disinformation measures can pose to human rights and the weakening of democratic structures — whether they are introduced by governments or corporations. Especially during the Covid-19 pandemic, it became apparent that “the legal and political abuse of what has been labelled the ‘fight against fake news’ has in some countries also resulted in reduced freedom of expression and political dissent” (Colomina et al., 2021: 16; see Commissioner of Human Rights of the Council of Europe, 2020).

---

30 While the precise requirements can depend on the specific context, in general „effective control” requires a demonstrable power to regulate and direct affairs in a particular area or over a particular entity. It is typically evaluated based on factors such as the ability to enforce laws, maintain order, make decisions, and respond effectively to changes or crises. In the context of state sovereignty and recognition, effective control helps to establish whether an entity qualifies as a state under international law (for a more detailed definition see, e.g., Hollis, 2021; Zwanenburg, 2020).
As Damjan Denkovski, Nina Bernarding, and Kristina Lunz show in the CFFP study “Power over Rights: Understanding and countering the transnational anti-gender movement”, the anti-gender movement around the world is much more than a “simple pushback against gender mainstreaming, the right to abortion, LGBTQIA+ rights, or sexuality education, or even the culmination of human rights proponents to realise human rights for all” (CFFP 2021a). It is “an increasingly transnational movement consisting of actors as diverse as the Catholic Church, governments, and right-wing think tanks shifting towards efforts to develop and produce alternative norms which are inimical to the concept of universal and indivisible human rights. […] What we are witnessing is a highly organised (but not centralised) well-funded, transnational movement working to undermine women’s rights, LGBTQI* rights, and civil society. These efforts are not about ‘gender’ as such, but it is about power and about maintaining or promoting social and political hierarchies in the face of their (perceived) decline. These efforts take place in the streets across the world, in local and national governments and at the international level. Human rights advocates and progressive governments, believing in the unstoppable and teleological progress of human rights, have spent too long not taking the threat seriously and not responding adequately” (ibid.).

A feminist approach to cybersecurity makes clear that (gendered) disinformation needs to be addressed and mitigated through human rights and intersectional feminist lenses. Malicious actors that weaponize gendered disinformation must be sanctioned, and states and corporations with control over the regulation of the spread of (dis-)information must be held accountable and live up to their (human rights) responsibilities. So far, women and other marginalized groups have been carrying the burden of their inactivity at the expense of their individual (human) security and (inter-)national peace and security.

“Gendered disinformation online reflects the existing gender or racial biases – but it is also a behavior modification machine, a very powerful one. It is part of the weaponization of the Internet.”
Kristina Wilfore, #ShePersisted

3.3 Feminist perspectives on data privacy and surveillance

Increasingly, both democratic and authoritarian regimes are engaging in large-scale data gathering, monitoring, profiling, and tracking of their citizens. Indeed, in its 2022 report, the Office of the UN High Commissioner for Human Rights highlighted “the very real and encroaching risk of creating systems of pervasive surveillance and control that may eventually choke the development of vibrant, prosperous and rights-respecting societies” (UN Human Rights Council, 2022c).

As Privacy International states, every human being is, to a degree, subject to government surveillance; thus, surveillance and data gathering can threaten everyone’s right to privacy (Privacy International, n.d.). However, as with every policy, or technologically enabled tool, surveillance and data gathering “reflect the political constellations in which [they are] embedded” (Akbari, 2022). In short, surveillance and data gathering not only reflect the sexist, racist, and ableist power relations present in our cultures but also risk consolidating gender and racialized power inequalities.

Encouragingly, increasing attention is being paid to surveillance’s impact on human rights other than the right to privacy. These include fundamental freedoms such as freedom of expression, public participation and the work of human rights defenders and journalists (Mijatović, 2023). Indeed, the report mentioned above by the UN High Commissioner for human rights focuses on the abuse of intrusive hacking tools (‘spyware’) by state authorities, which are often used “to clamp down on critical or dissenting views and on those who express them, including journalists, opposition political figures and human rights defenders.” The most prominent example of this spyware might be the Pegasus software. In 2022, Access Now and Front Line Defenders reported that “governments in the MENA region and beyond using the spyware to perpetrate human rights abuses and repress activists and journalists” (Access Now, 2022b). At least 85 human rights defenders were targeted, including many women rights defenders (UN Human Rights Council, 2022; ibid). As Access Now writes, “the impact of surveillance on women is particularly egregious and traumatizing given how governments have weaponized personal information extracted through spyware to intimidate, harass, and publicly smear the targets’ reputations.” (ibid).

Targeting human rights defenders is particularly harmful to those most marginalized as their rights depend on an active civil society (CFFP, 2021a). A match made in heaven: Patriarchy and surveillance

In addition to the fact that surveillance further marginalises those that fight for the rights of women

Info Box 2

Explainer: The anti-gender and anti-rights movement

As Damjan Denkovski, Nina Bernarding, and Kristina Lunz show in the CFFP study “Power over Rights: Understanding and countering the transnational anti-gender movement”, the anti-gender movement around the world is much more than a “simple pushback against gender mainstreaming, the right to abortion, LGBTQIA+ rights, or sexuality education, or even the culminated successes by human rights proponents to realise human rights for all” (CFFP 2021a). It is “an increasingly transnational movement consisting of actors as diverse as the Catholic Church, governments, and right-wing think tanks shifting towards efforts to develop and produce alternative norms which are inimical to the concept of universal and indivisible human rights. […] What we are witnessing is a highly organised (but not centralised) well-funded, transnational movement working to undermine women’s rights, LGBTQI* rights, and civil society. These efforts are not about ‘gender’ as such, but it is about power and about maintaining or promoting social and political hierarchies in the face of their (perceived) decline. These efforts take place in the streets across the world, in local and national governments and at the international level. Human rights advocates and progressive governments, believing in the unstoppable and teleological progress of human rights, have spent too long not taking the threat seriously and not responding adequately” (ibid.).

A feminist approach to cybersecurity makes clear that (gendered) disinformation needs to be addressed and mitigated through human rights and intersectional feminist lenses. Malicious actors that weaponize gendered disinformation must be sanctioned, and states and corporations with control over the regulation of the spread of (dis-)information must be held accountable and live up to their (human rights) responsibilities. So far, women and other marginalized groups have been carrying the burden of their inactivity at the expense of their individual (human) security and (inter-)national peace and security.

“Gendered disinformation online reflects the existing gender or racial biases – but it is also a behavior modification machine, a very powerful one. It is part of the weaponization of the Internet.”
Kristina Wilfore, #ShePersisted

3.3 Feminist perspectives on data privacy and surveillance

Increasingly, both democratic and authoritarian regimes are engaging in large-scale data gathering, monitoring, profiling, and tracking of their citizens. Indeed, in its 2022 report, the Office of the UN High Commissioner for Human Rights highlighted “the very real and encroaching risk of creating systems of pervasive surveillance and control that may eventually choke the development of vibrant, prosperous and rights-respecting societies” (UN Human Rights Council, 2022c).

As Privacy International states, every human being is, to a degree, subject to government surveillance; thus, surveillance and data gathering can threaten everyone’s right to privacy (Privacy International, n.d.). However, as with every policy, or technologically enabled tool, surveillance and data gathering “reflect the political constellations in which [they are] embedded” (Akbari, 2022). In short, surveillance and data gathering not only reflect the sexist, racist, and ableist power relations present in our cultures but also risk consolidating gender and racialized power inequalities.

Encouragingly, increasing attention is being paid to surveillance’s impact on human rights other than the right to privacy. These include fundamental freedoms such as freedom of expression, public participation and the work of human rights defenders and journalists (Mijatović, 2023). Indeed, the report mentioned above by the UN High Commissioner for human rights focuses on the abuse of intrusive hacking tools (‘spyware’) by state authorities, which are often used “to clamp down on critical or dissenting views and on those who express them, including journalists, opposition political figures and human rights defenders.” The most prominent example of this spyware might be the Pegasus software. In 2022, Access Now and Front Line Defenders reported that “governments in the MENA region and beyond using the spyware to perpetrate human rights abuses and repress activists and journalists” (Access Now, 2022b). At least 85 human rights defenders were targeted, including many women rights defenders (UN Human Rights Council, 2022; ibid). As Access Now writes, “the impact of surveillance on women is particularly egregious and traumatizing given how governments have weaponized personal information extracted through spyware to intimidate, harass, and publicly smear the targets’ reputations.” (ibid).

Targeting human rights defenders is particularly harmful to those most marginalized as their rights depend on an active civil society (CFFP, 2021a). A match made in heaven: Patriarchy and surveillance

In addition to the fact that surveillance further marginalises those that fight for the rights of women
Violating women’s reproductive rights

In May 2022, when the draft US Supreme Court Opinion that suggested that the court is set to overturn Roe v Wade was leaked, women in the US started to delete their period tracking apps from their phones “amid fears the data collected by the apps could be used against them in future criminal cases in states where abortion has become illegal” (Garamvolgyi, 2022). As The Guardian states, “in a state where abortion is a crime, prosecutors could request information collected by these apps when building a case against someone” (ibid).

While it is unclear what information period trackers would be required to share, experts warn that “without federal privacy standards in place to protect the personal information of users […] women are largely on their own when it comes to safeguarding sensitive health data that companies routinely collect” (Lima, 2022). In addition to period tracker apps, online health services, browser histories, and location data could be used by law enforcement to track down and prosecute those seeking abortion (ibid). Moreover, the risk of right-wing groups buying these data seems high, especially in states that encourage citizens to report and/or sue those seeking or performing abortions (ibid).

Policing women’s clothing

Azadeh Abkari, Assistant Professor at the University of Twente, has done extensive research on surveillance of women’s clothing in Iran by using traffic camera footage (Abkari, 2022). She states,” “in 2015, it was revealed that the entire country’s urban CCTV cameras transmit their footage to the headquarters of Special Police Forces, who are mandated to deal with insurgency. Soon after, suspicions were raised that data gathered through traffic cameras are used for other purposes such as controlling women’s hijab” (ibid.). At the beginning of April this year, media outlets reported that “police in Iran plan to use smart technology in public places to identify and then penalise women who violate the country’s strict Islamic dress code” (Agence France-Presse, 2023). After one warning, women will be taken to court. As Abkari writes, the ‘compulsory hijab and its vigorous enforcement (...) deprives women, fully or partially, from accessing public spaces (justice for Iran, 2014); limits their freedom of movement; affects their feeling of security and well-being in public (Gould, 2014); and gravely restricts their participation in different aspects of social life.’”

Understanding how smart mobility can reinforce gendered inequalities is particularly important as the debates around ‘smart cities’ continue to be based on either apolitical or semi-democratic political constellations. As Abkari (2022) writes, the ‘political systems in which smart cities are embedded’ receive too little attention, which neglects undemocratic and authoritarian visions for smart cities (ibid.).

Dismantling state-centric security narratives legitimising surveillance

These examples highlight the real-life consequences of data gathering and surveillance for marginalized communities in democratic and authoritarian states. Such consequences must be understood as symptomatic of policy developments shaped by gendered data and exclusive processes. They are the result of policies based on narratives of apolitical and neutral technological advancements and those that prioritize the state’s security interests over its citizens. In this state-centric militarised understanding, the insecurities experienced by women and other marginalized communities because of data collection are not important enough to act upon. In other instances, ensuring national security in the sense of regime survival leads to the surveillance of women in public spaces and, relatedly, to a violation of their rights and dignity.
4. What to do? Steps towards a true feminist cyber peace – policy recommendations

Building on the research and work of other feminist scholars and civil society actors, this policy brief advances the debate on feminist approaches to cyberspace and cybersecurity. It has been argued that existing state-centric discourses and policy approaches are either ill-suited to address the vulnerabilities faced by civil society and marginalized communities or actively undermine their security. It has also outlined clear components of a feminist approach to cyberspace and cybersecurity. One that aims for a positive cyber peace which renders everyone secure. However, this paper is by no means exhaustive. Further research is urgently needed, which also the recommendations reflect.

4.1 Policy Recommendations

1. Focus on a feminist understanding of cyberspace and cybersecurity in national and international cyber policies, norm-setting processes, and discussion fora.

- In cooperation with feminist civil society and organisations taking a human-centric approach that works for cyber peace at home and abroad, initiate an inclusive process that critically analyses and amends/replaces existing national cyber policies from an intersectional feminist perspective. Allow for a critical assessment of ‘blind spots’, for example, regarding the security of reproductive health data and crucial healthcare and support infrastructure for marginalized groups, such as trans or LGBTQIA+ people (see Block 3).

  - The design and implementation of this process should learn from previous or existing inclusive multistakeholder formats, such as those used in the development of Germany’s National Security Strategy (see German Federal Foreign Office, 2022a) or the German “Shaping Feminist Foreign Policy” guidelines (see German Federal Foreign Office, 2022b), and seek guidance from civil society and other stakeholders that have worked on inclusive, gender-responsive cybersecurity policymaking.³¹

- Ensure that (civil society) organisations advocating for a feminist understanding of security, disarmament, and arms control are taken seriously as important stakeholders and experts that must be involved in national and international cyber peace and cybersecurity negotiation fora and decisions. Integrate a regular multistakeholder consultation mechanism consisting of representatives from feminist civil society, the private sector, the technical community, and academia, for example, in the form of an advisory group, in national cyber and security strategies.

- Make sure that national cyber and security strategies do not silo gender-sensitive perspectives into one section but are gender-mainstreamed. Such strategies should be thought of and written from an intersectional feminist perspective from the start.

- Advocate for and promote gender-mainstreaming throughout the operative parts of the Programme of Action (PoA) (see WILPF, 2022), as well as in other international normative frameworks and cyber strategies, such as those of NATO and the EU.

---

³¹ Existing initiatives are, inter alia, the 2020 “Toolkit for Inclusive and Value-based Cybersecurity Policymaking” by Global Partners Digital (GPD), and the Association for Progressive Communication’s (APC) 2022 “Framework for Developing Gender-Responsive Cybersecurity Policy”.

4.1 Policy Recommendations

- Highlight the humanitarian and gender-specific dimensions and intersecting harmful impacts of cyber operations (including those against critical infrastructure, disinformation, large-scale data gathering, and surveillance) on marginalized groups and individuals based on their gender, race, ethnicity, and other markers of identity, to foster an intersectional feminist approach to cybersecurity and cyberspace in international and national policy debates and norm-setting processes.

  o Highlight the lived experience of marginalized communities affected by malicious cyber activities in policy documents and official statements on cyber security and cyber peace, including in national cyber strategies and international fora such as the Open-ended Working Group on the security of and in the use of information and communications technologies (UN OEWG) and the Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international Security (PoA), as part of a feminist advancement of the human rights-based and human-centric approach stressed in the resolution on the PoA (see UN First Committee, 2022).

  o Collect information about the lived experiences of marginalized communities with cyber operations, and make them a legitimate starting point for the design of international and national cyber norms and policies

    On a national level, initiate regular consultations with feminist civil society at home and abroad, for example, in the context of a newly established advisory group, as mentioned above

    On the international level, ensure the meaningful participation of feminist civil society not only in hearings about the inclusion of civil society in future meetings and conferences of the PoA but during negotiations “About the instrument's purpose, scope, form, and substance” (WILPF, 2022)

    On the national and international level, collect and evaluate data on the humanitarian impact of malicious cyber activities, such as cyber operations against critical infrastructure, surveillance, and (gendered) disinformation.

- Increase gender diversity as well as the staff’s gender-sensitivity in national and international discussion and negotiation fora on cyber policies and norms, for example, by setting up gender-diverse national delegations or expert panels for consultancy purposes, by establishing obligatory trainings, and by utilising “WPS National Action Plans or opportunities provided by other frameworks to advance women’s [and other marginalized groups’] participation within international cyber security” (Pytlak and Brown, 2020: 21).

- Acknowledge cyberspace as an additional sphere that needs to be addressed through the Women, Peace, and Security (WPS) Agenda in national cyber strategies and international fora such as the UN OEWG and the future PoA. Amend future WPS National Action Plans as appropriate (see the report “Gendering Cybersecurity through Women, Peace and Security” by Hofstetter and Pourmalek, 2023).

- Ensure that governmental or governmentally funded initiatives and projects on cybersecurity or cyber-capacity building at home or abroad (e.g., in the context of international assistance) are designed and implemented based on an intersectional feminist approach.

---

³² The resolution includes the following paragraphs in its preamble: “Underlining the importance of respect for human rights and fundamental freedoms in the use of information and communications technologies”, and “Highlighting the necessity of bridging digital divides, building resilience in every society and sector, and maintaining a human-centric approach”. The resolution is available here: https://digitallibrary.un.org/record/3991743/files/A_C.1_77_L.73-EN.pdf?ln=en.

³³ This recommendation is also part of the considerations on a gender-sensitive PoA, published by the Women’s International League for Peace and Freedom (WILPF) in their study “Advancing a Global Cyber Programme of Action” (WILPF, 2022).
2. Support feminist civil society to advance the debate and research about feminist cyber peace

- Support feminist civil society to further research on the militarisation of cyberspace and how to mitigate the latter in favour of feminist cyber peace, for example, by funding feminist research on the humanitarian (gendered) impacts of malicious cyber activities and the gender-sensitive design of cyber policies to overcome existing power inequalities and systems of discrimination.

- Support feminist civil society to shape and advance multilateral debates, such as within the frameworks of the UN OEWG and the PoA, for example, by granting yearly travel funds to feminist organisations.

3. Include and promote a feminist understanding of critical infrastructure in national cyber strategies, policies and international norms and norm-setting processes

- In official statements on the international and national level, as well as in the respective policies and political fora, make clear that critical infrastructure protection must protect those that these infrastructures serve, i.e., society and especially marginalized groups.

- In cooperation with feminist civil society, assess existing definitions of and policies on critical infrastructure (protection), and replace/reframe them in favour of an intersectional feminist understanding of critical infrastructure (protection) that centres on the lived experiences and needs of marginalized groups, and explicitly includes institutions and systems crucial to marginalized groups’ feminist security and enjoyment of human rights. This includes systems storing reproductive health data, medical and support centres for LGBTQIA+ people, or educational institutions and (child, elderly) care facilities.

- Rhetorically and formally integrate civil society, non-governmental organisations (NGOs), and humanitarian and development organisations as critical infrastructure in national and international cyber discourses and policies as they protect and advocate for democratic structures and human rights domestically and internationally. Politically and financially support initiatives mitigating cyber operations against the humanitarian, development, and civil society sector and those working towards enhanced cyber resilience and capacity-building for NGOs, such as the Humanitarian Cybersecurity Center (HCC) by the CyberPeace Institute.

- Initiate research programmes/funds and support existing efforts, for example, by the CyberPeace Institute, aiming at data collection on the humanitarian harm caused by cyber operations against critical infrastructures (as well as efforts to establish suitable methodologies/scales to evaluate cyber harm), in particular gender-disaggregated data, to legitimise and inform suitable national and international measures to enhance protection and resilience of such infrastructures.

- Politically and financially support existing for-profit and non-profit efforts on the national, EU, and international levels to fill the so-called “cyber skills gap” by, for example, including more women and non-binary people in the cybersecurity workforce to provide an increasing number of cybersecurity professionals needed, given that more sectors and entities are to be defined as ‘critical infrastructure’ according to a feminist approach. Ensure cybersecurity professionals are equipped to prevent and mitigate gendered cyber harm.
4. Ensure effective mitigation of (gendered) disinformation while protecting human rights and democratic structures, and provide support for victims of (gendered) cyber harm

- In official statements, (inter-)national debates, cyber strategies and policies
  - Condemn the use of (gendered) disinformation by state and non-state actors
  - Underline that today's social media companies' business model is a fundamental factor behind the immense spread of and harm caused by disinformation, and
  - Highlight the threat of gendered disinformation to democracy, media freedom, gender equality, human rights and national as well as individual security of especially marginalized communities, human rights advocates (women, non-binary, queer) policymakers and journalists.

- Regularly make gendered disinformation a point on the agenda of international fora, such as the UN OEWG, the future PoA, the EU, and NATO, and centre the lived experiences of groups or individuals affected by gendered disinformation, for example, by inviting them to expert hearings and consultations.

- In cooperation with civil society and academia, strengthen and improve existing regulatory approaches that combat disinformation, increase transparency in social media platforms' content moderation processes and outcomes, and hold the respective companies accountable, such as the European Services Act. Ensure that any approach to tackle disinformation is gender-sensitive and based on democratic values and human rights, and equally addresses gendered disinformation and includes rules for preventing (surveillance-based) advertising practices that profile marginalized groups.

- Replace and condemn international and national (cyber) norms, policies, or other regulatory practices that might unduly restrict the freedom of expression and the freedom to seek, receive and impart information, violate other human rights, impose large-scale surveillance and/or could be used against human rights advocates or journalists under the pretext of fighting (gendered) disinformation.

- Better control public funds that are used to spread state propaganda. Research has shown that in Slovenia, for example, funds from the EU and other public funds were used to support state and party propaganda (Pírková et al., 2021). Thereby, pay special attention to state propaganda weaponizing gendered disinformation on individuals, groups, parties, or initiatives aiming to promote human rights for all, such as the Istanbul Convention.

- Together with feminist civil society, the private sector, the technical community, and academia, establish a national support system for journalists, human rights defenders, policymakers, and other individuals or groups who are victims of (gendered) disinformation and (related) other forms of (gender-based) cyber harm and violence based on gender, race, or other markers of identity. Such a support system could be inspired, for example, by the Finnish Media Pool organisation. It may include the following components of support: an emergency helpline for psychological and other support, speedy intervention by the criminal justice mechanism, the attention of counterintelligence authorities, assistance with legal fees, physical security at home and work, cooperation with stakeholders involved to mitigate data leakages etc., and (depending on the actor responsible), diplomatic measures (Lucas, 2020: 10).

---

³⁴ Consider, e.g., the study “Informing the Disinfo Debate: A Policy Guide for Protecting Human Rights” (see Pírková et al., 2021) by Access Now, European Digital Rights (EDRi), and Civil Liberties Union for Europe. It outlines various policy recommendations especially for the European Union in terms of platform regulation, content moderation, etc. with the overall goal to protect human rights from disinformation.

³⁵ See Domen Savic's study “Spreading propaganda and disinformation using public funds. The case of Slovenia as a challenge for EU democracy” (2021, cited in Pírková et al. 2021).

³⁶ For more information on the Media Pool Organisation, see: www.mediapooli.fi/en/mission/.

³⁷ An inspiring example is Access Now’s 24h digital security helpline, operating in eight languages, that supports rapid-response emergency assistance for women and other marginalized groups under attack and draws attention to digital rights. For more information, see: https://www.accesnow.org/help/
4.1 Policy Recommendations

³⁸ Pay special attention to the mapping study “From Boots on the Ground to Bytes in Cyberspace” by Anne-Marie Buzatu (ICT4Peace Foundation) on the use of ICTs in security services provided by commercial actors that finds that “the capture, storage, analysis and utilization of a multitude of data points or information is intrinsically intertwined with security services and security provision, and that this information acquisition and instrumentalization in the information age in which we live impacts our enjoyment of human rights” (Buzatu, 2022: iv). To mitigate these issues, the study provides valuable policy recommendations such as identifying gaps in existing relevant norms and frameworks such as the Montreux Document, Wassenaar Arrangement, etc., and developing robust due diligence standards for the use of ICTs in the provision of security services by private actors, e.g., within the International Code of Conduct for Private Security Companies (ICoC) (ibid.: 51-53).

5. Ensure gender-sensitive arms exports for surveillance technology and make efforts to protect human rights and safeguard private information

³⁸– Collaborate with for-profit entities and feminist civil society organisations working on measures to counter (gendered) disinformation, gender-based online harassment/violence and other forms of online cyber harm based on gender or other identity markers. Support feminist civil society in their efforts through funds for research, awareness-raising, digital security trainings, and media and information literacy initiatives.

– Address and advance the debate about the risks emanating from existing and evolving ICTs that are used (or can be repurposed) by state and non-state actors (such as the private security sector)³⁸ for malicious surveillance and other large-scale data-gathering activities in and through cyberspace, especially for marginalized communities.

– Through naming and shaming and, ideally, legal mechanisms in fora like the UN Human Rights Council or the future PoA, sanction state and non-state actors using surveillance technologies to undermine human rights, fundamental freedoms, the freedom of the media, and democratic structures.

– Ensure that comprehensive gender-sensitive human rights and humanitarian law assessments are done before granting export licenses for surveillance and dual-use technology, including to EU, NATO, and NATO-equivalent countries.

   ° As a crucial aspect of conflict prevention, include this commitment in national guidelines and action plans, particularly the respective national Action Plans for the Women, Peace, and Security Agenda.

– In cooperation with feminist civil society, critically assess whether the export of surveillance technology not covered by the Wassenaar Arrangement or national regulations should be subjected to export control because of the risk of reinforcing gendered or racialized inequalities.

– Ensure to take full responsibility for survivors of online and offline gender-based violence facilitated by exported surveillance technology, both in peace and wartime (based on Bernarding et al., 2020), amongst others, by committing to victim’s assistance and efforts to (legally and financially) sanction the mis-/abuse of exported surveillance technology.
4.2 A note on advocacy for feminist cyber peace

We owe it mainly to the tireless and courageous work of (feminist) civil society and scholars that there has been an ever-growing body of literature, including policy recommendations focusing on human-centric, gender-responsive approaches to preventing, combating, and mitigating intersecting humanitarian cyber harm. We are thankful for and respect every single human rights and feminist advocate dedicating their energy and time to the cause of security for all, online and offline. To continuously advance feminist cyber peace, we would like to highlight two points: Firstly, we should never allow feminist perspectives to be neglected in ‘technical discussions’ or ‘techno-strategic expert discourses’. This is a well-known mechanism of conscious or unconscious exclusion in patriarchal spaces that feminists have already dismantled in other fields of foreign and security policy (for example, in nuclear policy; see the work by Carol Cohn and many others (see Cohn, 1987)). Cyber has many technical components, but, as this briefing has highlighted, they are always intertwined with non-technical dimensions, with humans, our rights, our political, social, and economic systems, and our digital and physical ways of life. Secondly, we should leverage this understanding to avoid thinking in silos and to get broader civil society on board. We should see it as a chance to find intersecting areas of cooperation, join forces, and show solidarity with civil society working in other fields and with movements with direct or indirect connections to cyber, such as the anti-nuclear weapons movement (e.g., the threat of cyber operations against a nuclear arsenal), feminist movements such as #MeToo (e.g., gendered disinformation, online gender-based violence), and the climate movement (e.g., disinformation about climate change).

4.3 A note on the role of the private sector

This policy briefing has advocated for a multistakeholder approach that actively includes the private sector. This comes with the challenge of ensuring initiatives and policies on all levels (national, international, EU) engage with the private sector in a way that does not harm marginalized communities and respects a feminist understanding of cyberspace and cybersecurity. As argued above, the private sector, and social media companies in particular, need to be held accountable for the detrimental impact of their business model on marginalized communities and thus regulated: they do not have any economic incentive to change their practices (such as surveillance-based advertising models or untransparent content moderation) themselves, and vulnerable groups have been paying the price of their political inactivity for years. To put it bluntly, it has always been unacceptable and, as empirical evidence shows, totally ineffective to make the human rights, freedoms and security of societies, especially marginalized groups, who interact online dependent ‘on the goodwill’ of the CEOs of social media companies or other private actors. Additionally, many critical infrastructures, as well as large parts of the ever-evolving ICT landscape in a broader sense, are privately owned and often also effectively controlled by private actors. The case of the war in Ukraine has underlined that public-private collaboration to mitigate malicious cyber operations can be a chance to better protect the rights and safety of civil society. For example, Starlink’s satellites provided Internet access (Tucker et al., 2022); and Microsoft has been supporting the Ukrainian administration and cyber defence in the fight against malware and other malicious cyber harms (Sanger et al., 2022). Besides, some private companies have made self-regulatory efforts, as seen with the ‘Cybersecurity Tech Accord’ – that is, however, not explicitly embedded in a human rights approach (see Brown and Esterhuysen, 2019; Cybersecurity Tech Accord, n.d.). Some private companies have also committed to several human-centric principles in cooperation with governments and civil society, for example, in the framework of the “Paris Call for trust and security in cyberspace” (Paris Call, n.d.). Nevertheless, companies must be pushed to enact more respect for human rights. They must be held accountable by states, for example, through the UN Guiding Principles on Business and Human Rights. “In addition to conducting human rights impact assessments to identify, understand, assess and address the adverse effects of their policies and practices on the enjoyment of human rights, they should be conducting cybersecurity due diligence to review the governance, processes and controls that are used to secure the information they process” (Brown and Esterhuysen, 2019).
5. Conclusion

This policy briefing started by noting the ongoing militarisation of cyberspace and its framing as a ‘hostile’ and ‘insecure’ environment, resulting in state-centric understandings of cybersecurity that reproduce (neo-)realist security paradigms. Using examples of cyber operations against critical infrastructure, (gendered) disinformation and online harassment, and data privacy and surveillance, it was argued that this state-centric, militarised understanding is ill-suited to address and mitigate the threats and vulnerabilities that civil society and marginalized groups face in and through cyberspace. Drawing from the existing work of feminist civil society and scholars, an intersectional feminist approach to cyberspace and cybersecurity was developed. This feminist understanding provided the basis for various actionable policy recommendations that this briefing has offered to (better) protect civil society and marginalized groups from cyber threats and to prevent and/or mitigate the related intersecting humanitarian impacts. By centring a feminist perspective on cyberspace and cybersecurity, this policy brief also illuminates pathways to broaden and advance the international debate on privacy and other human rights in cyberspace, to advocate for inclusive, gender-sensitive national cyber policies and robust norms of responsible state behaviour in cyberspace that are both grounded in international and international humanitarian and human rights law, fundamental freedoms, and democratic values.

We are fully aware that a feminist approach to cyber issues will not make the life of policymakers easier. It will instead put them in an uncomfortable position where complex solutions for complex issues must be found – which will likely cost more time and energy than ‘business as usual’ approaches informed by traditional security paradigms. However, states do have an obligation to protect their population and support a digital environment where everyone can communicate and interact freely and safely. In particular, those governments committed to a Feminist Foreign Policy must remain mindful of those most marginalized. They should become role models — by committing to a feminist understanding of cybersecurity and combating the militarisation of cyberspace. There will be material and rhetorical obstacles — feminists advocating for demilitarisation and cyber peace, too, have long faced rejection, ignorance, or even accusations of naivety. However, let us be clear: for decades, many had similar doubts that nuclear weapons could ever be reduced or even legally prohibited at all. In 2017, with the adoption of the Nuclear Ban Treaty (TPNW), civil society (especially the International Campaign to Abolish Nuclear Weapons) has shown the world otherwise. This success should be taken as an encouragement. There are opportunities to combat militarisation and pave the way for positive, feminist peace. One fundamental step is to change the perspective that we ‘tell the story’ from, as this will influence political (re-)actions and ‘imaginaries of future (im-)possibilities’⁴⁰ — which is precisely what this project has aimed to do. This briefing appreciates that it is part of an evolving discussion and will hopefully be the start of many more studies imagining a future where feminist cyber peace is possible. We hope it will be continuously advocated for, politically supported, and eagerly worked towards in a cooperative multistakeholder effort that leaves no one behind and aims to make everyone safe — offline and online.

⁴⁰ For valuable thoughts on “reassessing political possibilities”, see the article “Writing IR after COVID-19: Reassessing Political Possibilities, Good Faith, and Policy-Relevant Scholarship on Climate Change Mitigation and Nuclear Disarmament” by scholars Benoît Pelopidas and Sanne Verschuren (Pelopidas and Verschuren, 2023).
6. References


Association for Progressive Communications (APC) (2022) APC calls for Iran to immediately stop violence against citizens and blocking of internet access during the latest protests. APC. Available at: https://www.apc.org/en/pubs/apc-calls-iran-immediately-stop-violence-against-citizens-and-blocking-internet-access-during. [Accessed 20 March 2023].


CFFP (2021b) Power over Rights - Understanding and countering the transnational anti-gender movement, Volume II: Case Studies. CFFP. Available at: https://centreforffp.net/wordpress/wp-content/uploads/2023/01/PowerOverRights2_web.pdf [Accessed 8 June 2023].


Cillizza, C. (2021) 2 charts that show just how old this Congress actually is. CNN politics, ThePoint with Chris Cillizza. Available at: 2 charts that show just how old this Congress actually is | CNN Politics. [Accessed 11 June 2023].


HateAid (n.d.) Realität oder Fake? Bedrohung durch Deepfakes. HateAid. Available at: https://hateaid.org/deepfakes/. [Accessed 5 May 2023].


Internet Free and Secure Initiative (IFSI) (n.d.) A human rights respecting definition of cybersecurity. IFSI. Available at: https://freeandsecure.online/definition/. [Accessed 12 March 2023].


References


United Nations First Committee (2022) Resolution on a Programme of action to advance responsible State behaviour in the use of information and communications technologies in the context of international security. United Nations General Assembly.


AUTHORED BY: Nina Bernarding and Vivienne Kobel

CONTRIBUTORS: Allison Pytlak (The Stimson Center), Kamilia Amdouni (CyberPeace Institute), Anne-Marie Buzatu (ICT4Peace), Azadeh Akbari (University of Twente, Netherlands), Eliska Pírková (Access Now), Damjan Denkovski and Anna Provan (both CFFP).

EDITING: Katie Washington

DESIGN: Leitmotiv.studio, Nathanael Dehn, (Mathildenstraße 10, 12459 Berlin)

The publication was financially supported by: Microsoft