# Gender approaches to cybersecurity: design, defence and response

Millar, K.; Shires, J.; Tropina, T.

# Gender approaches to cybersecurity: design, defence and response

KATHARINE MILLAR | JAMES SHIRES | TATIANA TROPINA

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

www.unidir.org

# Gender approaches to cybersecurity: design, defence and response

# Acknowledgements

Support from UNIDIR core funders provides the foundation for all of the Institute's activities. The Gender and Disarmament programme is supported by the governments of Germany, Ireland, Norway, Spain, Sweden and the United Kingdom.

The authors would like to gratefully thank the following people and organizations for their generous feedback, time and expertise in supporting this research and reviewing this report.

- **Marwa Azelmat**, Association for Progressive Communications
- **Winnona DeSombre**, Google
- **Avri Doria**, Technicalities
- **Eugenia Dorokhova**, Geneva Centre for the Democratic Control of the Armed Forces
- **Serge Droz**, Forum of Incident Response and Security Teams
- **Verónica Ferrari**, Association for Progressive Communications
- **Lenka Filipová**, United Nations Institute for Disarmament Research
- **Noelia Garcia Nebra**, International Organization for Standardization
- **Joyce Hakmeh**, Chatham House
- **Renata Hessmann Dalaqua**, United Nations Institute for Disarmament Research
- **Louise Marie Hurel Silva Dias**, Department of Media and Communications, London School of Economics
- **Aiko Holvikivi**, London School of Economics Centre for Women, Peace and Security
- **Jaana Holvikivi**, Helsinki Metropolia University of Applied Sciences
- **Edward Humphreys**, Convenor of the ISO/IEC Joint Technical Committee SC 27/WG 1

- **Andraz Kastelic**, United Nations Institute for Disarmament Research
- **Franziscka Klopfer**, Geneva Centre for the Democratic Control of the Armed Forces
- **Catalin Marinescu**, International Telecommunication Union
- **Beatrice Martini**, Access Now Digital Security Helpline
- **Niels ten Oever**, University of Amsterdam
- **Christine Runeggar**, Internet Society
- **Toby Shulruff**, National Network to End Domestic Violence
- **Julia Slupska**, University of Oxford
- **Leonie Tanczer**, University College London
- **Tracy Tuplin**, International Telecommunication Union
- **Kerstin Vignard**, United Nations Institute for Disarmament Research
- **Julia Voo**, Harvard Kennedy School
- **Daniel Woods**, University of Innsbruck

# Notes

The designations employed and the presentation of the material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries. The views expressed in the publication are the sole responsibility of the individual authors. They do not necessarily reflect the views or opinions of the United Nations, UNIDIR, its staff members or sponsors.

# Citation

Millar, Katharine; Shires, James; and Tropina, Tatiana. 2021. Gender Approaches to Cybersecurity: Design, Defence and Response. Geneva, Switzerland: United Nations Institute for Disarmament Research. https://doi.org/10.37559/GEN/21/01

# About UNIDIR

UNIDIR is a voluntarily funded, autonomous institute within the United Nations. One of the few policy institutes worldwide focusing on disarmament, UNIDIR generates knowledge and promotes dialogue and action on disarmament and security. Based in Geneva, UNIDIR assists the international community to develop the practical, innovative ideas needed to find solutions to critical security problems.

# About the Gender and Disarmament Programme

The Gender and Disarmament programme seeks to contribute to the strategic goals of achieving gender equality in disarmament forums and effectively applying gender perspectives in disarmament processes. It encompasses original research, outreach activities and resource tools to support disarmament stakeholders in translating gender awareness into practical action.

# About the authors

**Dr. Katharine Millar** is an Assistant Professor of International Relations at the London School of Economics and Political Science (LSE) and holds a doctoral degree from the University of Oxford, United Kingdom. Her research interests lie in the relationship between gender, sexuality, politics and violence. Her current research examines gender and cybersecurity; gender, race, militarism, and contemporary populism(s); and the transnational components of death associated with COVID-19. Dr. Millar is a member of the Millennium journal Board of Trustees and of the Centre for Women, Peace and Security at the LSE. She has participated in consultation processes regarding the United Nation's Women, Peace and Security Agenda for several national governments and international organizations, including the United Kingdom, Canada and the North Atlantic Treaty Organization (NATO).

**Dr. James Shires** is an Assistant Professor with the Institute of Security and Global Affairs at the Leiden University, the Netherlands, and a fellow with the Cyber Statecraft Initiative at the Atlantic Council. He is also a Research Affiliate with the Centre for Technology and Global Affairs at the Department of Politics and International Relations, University of Oxford. He holds a DPhil in International Relations from the University of Oxford. His research examines cybersecurity governance, focusing on the interaction between threats to individuals,

States and organizations, new international political dynamics, and the development of cybersecurity expertise. He has won awards from the Hague Program on Cyber Norms, the German Marshall Fund and the International Institute for Strategic Studies (IISS).

**Dr. Tatiana Tropina** is an Assistant Professor in Cybersecurity Governance with the Institute of Security and Global Affairs at Leiden University and holds a doctoral degree from the Far Eastern Federal University, Russia. Her areas of expertise include international standards to fight cybercrime, digital investigations, self- and co-regulation to address cybersecurity issues, and the multi-stakeholder approach to cybersecurity. She has been involved in both legal research and applied cybercrime and cybersecurity projects, such as cybercrime studies for the Global Symposium of Regulators (2010) and the United Nations Office on Drugs and Crime (2012–2013), research on illicit financial flows and digital technologies for the World Development Report 2016, and a project with the German Federal Criminal Police Office on improving mutual legal assistance on interception of electronic communications in the European Union (2015–2018).

# Table of Contents

# List of Abbreviations

| | |
|---|---|
| **AI** | Artificial intelligence |
| **CERT** | Computer Emergency Response Team |
| **IEC** | International Electrotechnical Commission |
| **IETF** | Internet Engineering Task Force |
| **ICT** | Information and communications technology |
| **ISO** | International Standards Organization |
| **IT** | Information technology |
| **ITU** | International Telecommunication Union |
| **LBGTQ+** | Lesbian, gay, bisexual, transgender and queer people and people of diverse gender identities, gender expressions and sexual orientations |
| **OEWG** | Open Ended Working Group |
| **SDG** | Sustainable Development Goal |
| **STEM** | Science, technology, mathematics and engineering |

# Executive summary

Multilateral processes on cybersecurity have recently begun to include official statements drawing attention to its gendered dimensions. Several delegations participating in the United Nations Open Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security have stated the need for gender mainstreaming into cyber norm implementation and gender-sensitive capacity building, as well as a better understanding of the linkages between cybersecurity and gender equality frameworks. However, questions remain about the overall application of gender perspectives to cybersecurity, as well as what kinds of action are needed to effectively implement a gender approach to cybersecurity and turn those goals into reality.

To tackle this knowledge gap, this report outlines the relevance of gender norms to cybersecurity. It draws on existing research, supplemented by stakeholder and expert interviews, to assess gender-based differences in the social roles and interaction of women, men and non-binary people of all ages reflected in the distribution of power (e.g. influence over policy decisions and corporate governance), access to resources (e.g. equitable access to education, wages or privacy protections), and construction of gender norms and roles (e.g. assumptions regarding victims and perpetrators of cyber-facilitated violence).

Overall, gender norms inform cybersecurity in two ways. First, gender constructs individual identities, roles and expectations within cybersecurity and broader society, such as the frequent association of technical expertise with men and masculinity. Second, gender operates as a form of hierarchical social structure. This means that activities and concepts associated with masculinity, such as technical expertise, are often, but not always, valued over those associated with women and femininity, such as communications expertise or equality, diversity and inclusion initiatives.

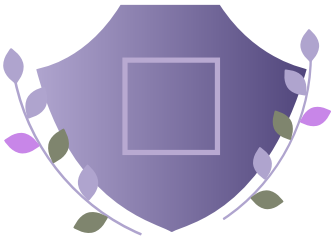
To understand how gender shapes specific cybersecurity activities, this report proposes a new cyber-centric framework based on the three pillars of design, defence and response, aligned with prevalent perspectives among cybersecurity practitioners and policymakers. In each of these three pillars, the research identifies distinct dimensions of cyber-related activities that need to be considered from a gender perspective.

## Design

Technology design is gendered: it misunderstands, omits and consolidates certain gendered uses, privileges perceived masculine practices over feminine ones, and essentializes femininity in problematic ways. Cybersecurity design inherits these issues. The threat models, reporting and user-control procedures, and advertising of cybersecurity technologies mean that women are more likely to have cybersecurity threats downplayed or omitted; more likely to have additional security burdens; and more likely to be affected by disingenuous cybersecurity marketing.

## Defence

Defensive threat simulations and characterizations often involve gender stereotyping. More deeply, how we think about defence – that is, what it means to defend and the common-sense actions we take to defend – reflects a series of norms associated with masculinity, such as protection, technical competence and autonomy. Gender norms around vulnerability can make admitting error, seeking help or working cooperatively more difficult, generating reluctance to actively pursue cybersecurity defence or exercise transparency.



## Response

Cybersecurity responses involve distinct gender dynamics. The priorities, composition, expected practices and working hours, and workplace culture of incident-response teams require gender analysis. Furthermore, the informality of cybersecurity response communities – often composed of close trust networks formed through years of interaction – means that they may have lower participation from women and minoritized groups, even when adjusted for overall proportions in the industry. Cybersecurity responses can also involve a gendered dynamic of victim-blaming,

wherein organizations or individuals with insufficient cybersecurity defence or identity-protection measures are perceived as "asking to be hacked".

Research addressing the linkages between gender and cybersecurity is sparse, although growing. Thus, in each of these pillars, the report outlines areas for further investigation. This report also proposes recommendations for the incorporation of gender considerations throughout international cybersecurity policy and practice, including:

» Cybersecurity standards have an important role to play in the development of gender-sensitive technology design. Standards makers should assess the extent of gender equality in cybersecurity standards, including meaningful participation, standards content and language, and direct and indirect gender effects. The first step towards this is the collection of gender-disaggregated data throughout cybersecurity policy and practice.

» Efforts to address the gender gap in cybersecurity should build on broader moves to increase women's participation in science, technology, engineering and mathematics (STEM). Additionally, it is important to raise the profile and value of cybersecurity skills and expertise beyond STEM (e.g. communications, ethics, legal governance). All cybersecurity stakeholders should counter harmful gendered perceptions and stereotypes, and they should support organizational and cultural shifts that value diverse activities and capacities.

» Cybersecurity legal measures should incorporate a gender perspective into the development, implementation, oversight and evaluation of

relevant laws. Legal measures should be underpinned by open and participatory legislative process involving all stakeholders, especially civil society groups and organizations promoting the rights of individuals of underrepresented and marginalized gender identities.

» All organizations – in both the public and private sectors – should conduct "gender and cybersecurity" training for practitioners and policymakers. This training should incorporate a dual focus on (a) gender equality, diversity and inclusion in the workplace and (b) the development of a gender perspective on cybersecurity as a professional skill. This training will provide a practical introduction to gender as an element of policy, ensuring that gender expertise is a foundational and respected aspect of cybersecurity professional practice and policymaking.

» States participating in UN cybersecurity processes could support and fund the development of a cyber and gender training toolkit and require public sector organizations and private sector contractors to use it where possible. Non-state actors in academia and, particularly, civil society could contribute expertise in toolkit development, while corporate actors could implement modified versions and use commercial leverage to ensure others do so as well. States could also use the toolkit to build inter-State cooperation on cybersecurity.

Such measures would ensure that cybersecurity improves the security of people of all gender identities and expressions, as well as international peace and security. The ultimate conclusion is that these two levels of security cannot be separated.

# 1. Introduction

Gendered dynamics and assumptions are prevalent in the field of cybersecurity. Many cybersecurity threats are experienced differently by women and girls, men and boys, and people of non-binary gender identities.[1] People of different genders also participate unequally in the formation and enactment of cybersecurity policies and practices.[2]

However, it was only recently that multilateral processes on cybersecurity started to include official statements drawing attention to the gendered dimensions of cybersecurity governance.[4] Notably, several delegations participating in the UN OEWG on developments in the field of ICTs in the context of international security have stated the need for gender mainstreaming into cyber norm implementation and gender-sensitive capacity building, as well as a better understanding of the linkages between cybersecurity and gender equality frameworks.[5]

Despite these developments, existing research on gender and cybersecurity is sparse. This is partly

## gender

Gender refers to the socially and culturally constructed roles, behaviours and attributes associated with masculinity and femininity in a given time and place. Gender norms are changeable over time; they inform individual identities, social relations, and the distribution of resources and power in society. Although gender is often socially understood as expressing expectations regarding appropriate behaviour for men and women, gender is non-binary and diverse. It refers to people of all gender identities and expressions.[3]

due to the common misperception that the technical or technological aspects of cybersecurity are gender-neutral, and therefore gender-blind, without different effects for individuals of marginalized gender and sexual identities and expressions (and other minoritized groups).[6] It is also arguably due partially to the constant, iterative change within the field, which encourages experts to prioritize addressing new risks rather than evaluating the gendered implications of cybersecurity practices.

To tackle this knowledge gap, this report explores cybersecurity issues from a gender perspective. Specifically, the research answers the following questions:

» What are the main gendered implications of cybersecurity policies and practices?

» How are these implications addressed in current research and policy?

» What further actions would address gendered inequalities and differential harms in cybersecurity?

The report answers the first research question by developing, in chapter 2, a new, cyber-centric framework, aligned with prevalent perspectives on cybersecurity among practitioners and policy makers. This framework is used to organize and analyse the gendered implications of cybersecurity systems, processes and practices in three pillars: design, defence and response. Each pillar is then discussed separately in chapters 3–5, which outline the content of the pillar and the broad, sector-level gender dynamics at work within it.

To answer the second research question, the discussion of each pillar also contains a more detailed analysis of an illustrative case study:

cybersecurity standards, talent and expertise, and legal measures. To assist policy makers and practitioners in identifying the gender and equality implications of technical components of cybersecurity, we answer the third research question by highlighting key areas for further research; providing a framework for structuring and synthesizing this future work; and developing concrete policy recommendations. In so doing, we hope to improve international cybersecurity by reducing the negative consequences of gendered assumptions, biases and omissions.

## gender equality

Gender equality is the principle that "women and men, girls, boys [and non-binary people] have equal conditions, treatment and opportunities for realizing their full potential, human rights and dignity, and for contributing to (and benefitting from) economic, social, cultural and political development".[7]

# 2. Cybersecurity and gender

This report defines cybersecurity as the prevention and mitigation of malicious interference with digital devices and networks. Malicious interference, in turn, is defined as illegitimate intrusion into or disruption of the functioning of digital devices and networks.[8]

This definition is actor-agnostic. Intrusion and disruption can be part of State-sponsored activities, including sabotage and espionage. However, States are far from the only actors performing intrusion and disruption. Financially motivated cybercriminals probably represent the vast majority of intrusions, while a range of non-State actors regularly disrupt digital activities.[9]

As this definition is narrower than some others, we note two important qualifications. First, this definition does not include general threats or risks posed by emerging technologies, such as artificial intelligence (AI), unless such technologies are used to enable or amplify intrusion and disruption.[10] AI, including the generation of "deepfake" text, image or video content, is not per se a cybersecurity issue.

Second, this definition does not include concerns about content. The question of whether the spread of undesirable content online is a cybersecurity issue has a contested history. Many experts have commented on a split between supporters of "like-minded" (or "multi-stakeholder") perspectives in cybersecurity, who do not include content concerns in their conception of cybersecurity, and opponents of this view, often loosely and simplistically grouped together under the term "cyber-sovereignty".[11] This split, however, has narrowed in recent years, as "like-minded" States have prioritized content concerns under the label of "disinformation" or "influence/information operations".[12]

There are overlaps between content concerns and malicious interference as defined above, not least in "hack-and-leak" operations.[13] Consequently, in this report we include content issues relating to gender, such as "revenge porn" (the non-consensual publication of intimate photos or videos), where there is an element of malicious interference involved in obtaining that information.[14]

These overlaps notwithstanding, we recognize that the issues above – AI,[15] deepfakes[16] and disinformation[17] – have gendered impacts. Similarly, trolling, bullying and harassment on social media are clearly gendered and a pressing social and policy problem.[18] Although these issues are vitally important, they do not necessarily involve malicious interference with digital devices and networks, and so they are not examined here.

Our definition of cybersecurity itself has gendered implications,[19] as it begins from the security of networks, devices and systems, rather than individuals of marginalized gender and sexual identities and expressions (and other minoritized groups). Beginning with the individual – particularly women – is highly effective in demonstrating the relevance of digital technologies to existing gender dynamics and

## gender informs cybersecurity in two key ways

First, gender constructs individual gender identities, roles and expectations within cybersecurity and broader society – such as frequent association of technical expertise with men and masculinity.

Second, gender operates as a form of hierarchical social structure. This often, but not always, means that activities and concepts associated with masculinity – such as technical expertise – are valued over those associated with femininity, such as policy expertise or equality and diversity initiatives.[21]

hierarchies. However, it is less effective in demonstrating the ways in which seemingly gender-neutral "technical" choices – in technological design, daily practice and regulation – are, in fact, themselves built on gender hierarchies, assumptions and inequalities (and often inadvertently produce new ones). We therefore begin with this more technical element of cybersecurity and work outwards, to examine its gendered assumptions and effects on individuals.[20] By doing so, we hope to speak to current cybersecurity policy makers and practitioners in familiar language; reveal the gender implications of seemingly gender-neutral technologies and practices; and assist practitioners and policy makers in developing this gender perspective themselves.

## 2.1 The three-pillar framework

The framework for analysing gender and cybersecurity that we use in this report has three pillars.

### Pillar 1. Design

The design pillar of cybersecurity aims to build security into socio-technological systems. This reduces attack surface area and prevents whole classes of vulnerability or attack vector. It also incentivizes or requires individuals and organizations to act in ways that increase, rather than decrease, their security. This pillar seeks to prevent and mitigate malicious interference in a highly anticipatory way, usually by modelling threats and designing against those models.

### Pillar 2. Defence

As achieving "perfect" cybersecurity design is impossible, the defence pillar concerns strategies to reduce risk, identify vulnerabilities and ameliorate potential harms after systems have been designed and implemented. The defence pillar of cybersecurity aims to anticipate, detect, identify and neutralize more specific threats of interference and disruption to digital devices and networks.

### Pillar 3. Response

As cybersecurity defence is a question of risk management, there will always be cybersecurity incidents: successful intrusions into or disruption of digital devices and networks. The last pillar of cybersecurity concerns how States respond to these incidents. This includes post-incident investigation and recovery; legal measures to punish and deter perpetrators; limiting the spread of incidents through information sharing; and compensation for those affected.

This framework aligns closely with prevalent conceptions of cybersecurity in professional and expert communities. These communities generally see the purpose of cybersecurity as preventing intrusion and disruption, in line with the narrow definition of cybersecurity above.[22] Moreover, these three pillars resonate with common concepts in these communities, such as "security by design" (pillar 1), "cybersecurity defence" measures (pillar 2) and "incident response" (pillar 3). The cyclical "workflow" structure of these pillars – moving from design via defence to response (and back to (re)design) – is hopefully also intuitive to practitioners who use similar frameworks to structure and prioritize their plans and operations.

This broad framework is intended to be exhaustive, in that all cybersecurity actions fit into at least one of these pillars. Given its simplicity, there are areas of overlap. It is not always easy to decide where design ends and defence begins, as more adversarial cybersecurity defence (protecting particular targets against specific threat actors) can be assisted or even rendered unnecessary by good cybersecurity design. Defence and response also overlap because – as the well-known cyber "kill chain" illustrates – cyber-intrusion or disruption is a multistage process, and each stage can be addressed separately.[23]

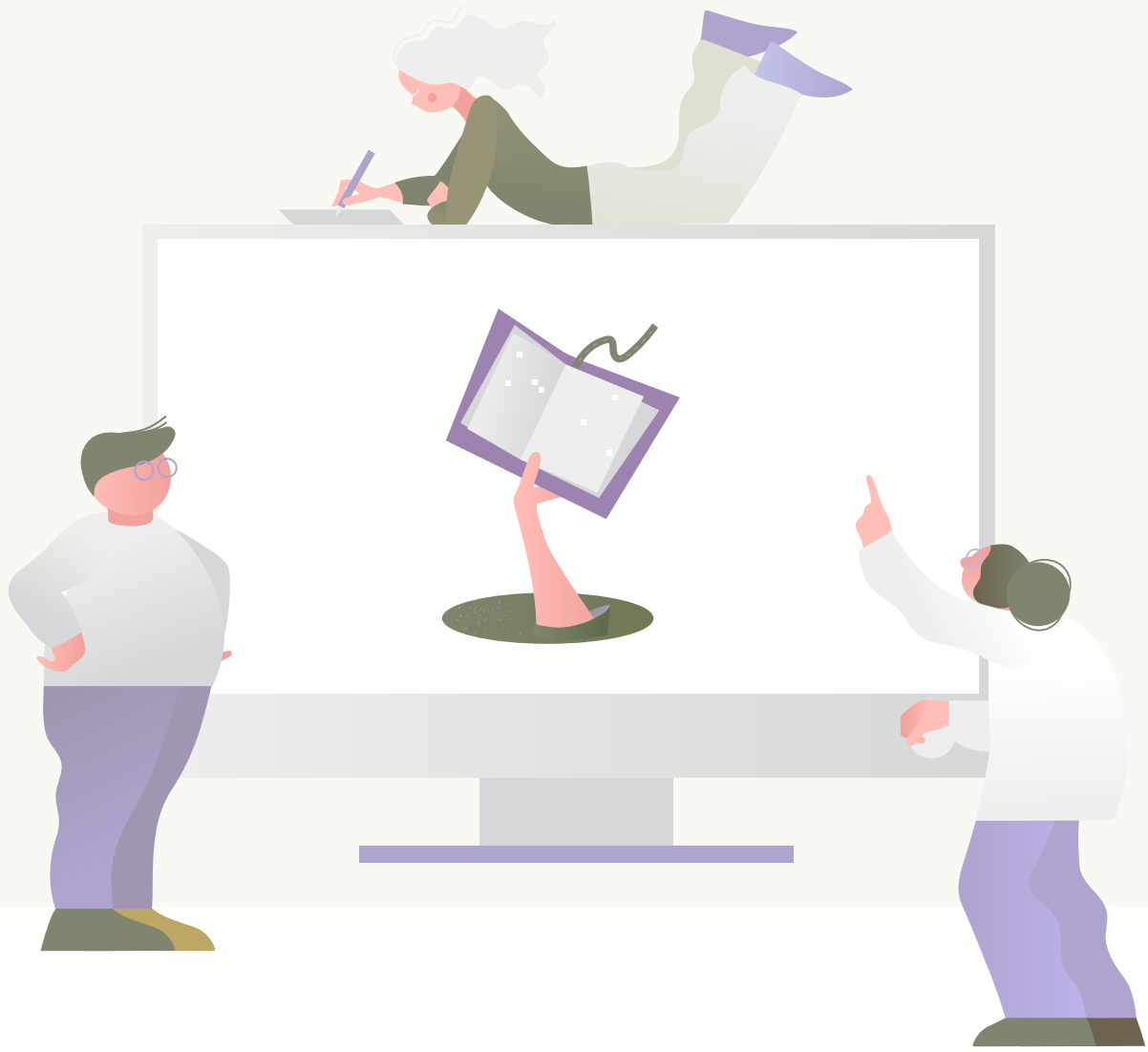
Finally, the three-pillar framework straddles norm implementation and capacity building. Capacity-building – including State and non-State cybersecurity capacity – involves improvement across design, defence and response, while the 11 norms of responsible State behaviour endorsed by the United Nations General Assembly by consensus in 2015 can also be implemented through actions in cybersecurity design, defence and response.[24]

In the following chapters, we provide a gender perspective on each pillar of cybersecurity in turn, focusing on three case studies: cybersecurity standards, talent and expertise, and legal measures (see Table 1). The case studies were chosen because they capture existing research and policy on gender; they offer the opportunity for specific recommendations to current cybersecurity processes; and they are key to norm-implementation and capacity-building.

# Table 1. The three-pillar framework of cybersecurity

| Pillar | Case study | Other elements (non-exhaustive examples) |
|---|---|---|
| Design | Standards | Research<br>Threat modelling<br>Developing end-user guidance |
| Defence | Talent and expertise | Preparation and protection<br>Threat monitoring<br>Insurance and liability |
| Response | Legal measures | Incident response<br>Information-sharing (for mitigation)<br>Insurance and compensation |

# 3. Design



Over and above the specific context of cybersecurity, technology design is gendered: it misunderstands, omits and consolidates certain gendered uses, it privileges perceived masculine practices over feminine ones, and it stereotypes femininity in problematic ways.[25] These gendered aspects have direct impact on cybersecurity. Many technology designers are aware of the gendered implications of their work, and there are entire sub-disciplines, including user experience and user-centred design, that seek to improve technology design along gendered lines.[26] The following are select examples of gendered technology design:

» Virtual reality prototypes have, like many technologies, omitted women almost entirely as their intended users.[27]

» The choice of women voice assistants for phones, smart speakers and devices, and satellite navigation has been shown to reinforce harmful assumptions about gendered power relationships.[28]

» The design of technologies directly marketed to women, known as "femvertizing", often "prey[s] on women's assumptive need to correct problematic behaviors or unacceptable physical deviancies".[29] Gendered assumptions about what is "normal" are deployed in advertising material to encourage women to purchase products that enable them to conform or minimize "abnormal" physical and personal characteristics.

» There are gendered differences in academic and industry research on technology, as in other fields, including in citation practices.[30]

These broader gendered aspects of technology design influence cybersecurity in several ways. Most basically, the conception of cybersecurity employed in technological design is gendered. For example, the design of smart household devices has not adequately included intimate partner violence in the "threat modelling" phase of design, meaning that supposedly secure smart devices increase gendered risks.[31]

Even services designed to prevent this problem, such as online resources about leaving abusive relationships, can themselves be a risk to individuals if the abuser discovers the tool. Therefore, the designers of such tools – such as emergency "exit" buttons on the websites of victim organizations – have to take these risks into account in their threat models.[32] To reduce the occurrence of these inadvertently dangerous blind spots, it is thus important that the design and threat-modelling processes include diverse perspectives and people from minoritized groups.[33]

Another example can be found in contemporary cybersecurity measures aimed at protecting individuals from privacy breaches or identity theft, which rely on the use of personal information as the backup for passwords and online account access. These assume that the "bad actor" is a stranger without other access to the middle name of a parent or the name of a first pet – an assumption not met in instances of intimate partner and family violence.[34] The design of online identity-verification procedures thus has gendered effects due to the conception of "threat" they employ (and, in this case, omit).

The burden of cybersecurity work is also gendered. Privacy settings on social media are more likely to be activated by women, especially for images.[35] Women are expected to exercise near-total control over their own digital footprint (such as changing passwords and deleting social media accounts, etc.) in order to reduce their vulnerability to digital coercive control.[36] Failing to act as a perfect digital user – due to a lack of time or literacy, or a reliance on technology for support and social connections – becomes a source of victim-blaming.[37] There is also a trade-off here between different cybersecurity goals: permitting companies to design applications that access location and other data can be a way of preventing other privacy threats, even though the companies use this data commercially, which can itself be a threat.

Finally, the advertising of cybersecurity technologies is gendered. Software that can remotely monitor phones and other devices is marketed as designed for child protection, enabling families to track the movements of their children online.[38] But this software is also used in situations of intimate partner violence (and is often termed "stalkerware").[39] Google has banned all advertising of stalkerware to combat this dual-use problem.[40]

Overall, cybersecurity design inherits the gendered omissions, biases and reinforcement of gendered assumptions that are evident in technology design. The threat models, reporting and user-control procedures, and advertising of cybersecurity technologies mean that women (or the most vulnerable gender groups in a particular context) are more likely to have cybersecurity threats downplayed or omitted; more likely to have additional security burdens; and more likely to be affected by disingenuous cybersecurity advertising.

## 3.1 Case study: cybersecurity standards

Cybersecurity design and implementation are governed by a wide range of direct and indirect standards, aiming to make digital technologies

### gender- sensitive and inclusive

Gender-sensitive policy and programmes are aware of and address gender differences in the way people are affected by policy. Gender inclusive policy-making refers to the use of language, decision-making procedures and other practices that proactively support the equal participation and influence of people of all gender identities and expressions.[46]

compatible with goals on quality, ethics, safety, integrity, availability and sustainability, among others. A standard provides "rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context".[41] Standards, as highly codified but voluntary documents, are a middle ground between mandatory technical regulations and broader "best practices".[42]

Standards cover a wide range of issues across all three pillars of our framework. However, the creation of standards is itself part of the design process, seeking to structure the wider cybersecurity environment rather than defending against or responding to specific threats.

Cybersecurity-specific standards are both public and private and are put forward by a variety of bodies: national standards bodies such as the United States National Institute of Standards and Technology (NIST), international organizations such as the International Standards Organization (ISO), the International Electrotechnical Commission (IEC) and the International Telecommunication Union (ITU), technical governing bodies such as the Internet Engineering Task Force (IETF), or industry- and sector-specific associations or non-governmental advocacy organizations.[43]

## gender analysis

Gender analysis requires the systematic gathering and examination of empirical data on gender differences and social relations in context in order to identify and understand inequities and social structures based on gender (and other important forms of social and cultural power). It is the basis for gender-responsive policy-making.[50]

International standards bodies have recognized that they need to be "gender-sensitive" – that is, aware of differential impacts according to gender – and "gender-responsive" – that is, driving a more inclusive standards-development process that incorporates different gender perspectives, addresses gender inequalities and, ideally, empowers women and girls.[44] The ITU created its Women in Standardization Expert Group as part of its efforts to achieve the United Nations Sustainable Development Goal (SDG) 5 on gender equality and women's empowerment.[45]

In 2019, the United Nations Economic Commission for Europe (UNECE) published a declaration on "Gender Responsive Standards and Standards Development", signed by more than 50 standards-developing organizations. It outlined three groups of actions:

1. Working towards gender balanced, representative and inclusive standards-development environments;
2. Creating gender-responsive standards; and
3. Creating gender-responsive standards bodies.[47]

Following that declaration, the ISO developed a Gender Action Plan that includes participation in standards development; participation in standardization bodies; and gender-sensitive standards content.

These initiatives provided a more structured approach to existing research on the gender impact of standards. Canonical examples of standards revision following gender analysis include car safety standards (where seatbelts and crash tests are designed for the average male body weight and size) and efficiency standards for office air conditioning (which were based on metabolic rates of men and significantly overestimated women's metabolism).[48] Research has also identified other standards, especially

those relating to United Nations SDGs, such as textile supply chains or clean cooking equipment, that have a differential impact on women due to their greater role in, and disproportionate time spent on, these activities.[49]

To consider the gendered implications of cybersecurity standards, we focus on the 27000 series developed by the ISO and the IEC and published in two iterations, in 2005 and 2013.[51] The ISO 27000 series is a family of mutually supporting information security management standards that "can be combined to provide a globally recognised framework for best-practice information security management".[52] We use the example of the ISO due to its global influence and wide recognition, although the discussion could apply equally to other standards and organizations.[53]

It is difficult to assess gender participation in the historic development of the ISO 27000 series, as this includes external advice and consultation. The current ISO 27000 committee, however, is beginning to collect data on the number of men and women involved in the various projects under this committee, including absolute ratios of men and women but also ratios in different roles and at different levels (e.g. project editors) and geographical and national member distribution.[54]

This gender analysis of participation in the development and management of the ISO 27000 series is vital as it seeks to ensure that a diverse range of views are recognized in the creation of standards and in the management and operation of standards organizations. However, it is only a first step. Following the expansive definition of gender equality introduced above, further analysis should consider whether participation is meaningful and effective in implementing change.[55]

Furthermore, efforts to analyse (and, if necessary, expand) participation must be accompanied by a gender analysis of the content of standards.

Thus far, ISO 27000 cybersecurity standards have been dominated by an assumption that they are generic and therefore gender-neutral, in line with broader trends in technological design noted above.

ISO stakeholders did note one example of gendered language in the 27000 series that was subsequently changed. Several years ago, the term "housekeeping" was flagged by women participating in discussion of standards revision as inappropriate due to its gendered connotations: although, in cybersecurity, housekeeping refers to the process of hard drive space optimization, outside cybersecurity, housekeeping is a category of feminized work that is frequently under-rewarded or omitted by labour analyses.[56] The term was subsequently removed and replaced by more neutral language.[57] A thorough analysis of the content of the 27000 series, including not just gendered language but also gendered effects (e.g. through assumptions around users and relevant risks) may identify further instances.

The current work on the 27000 series also highlights that standards development must address issues of both content and participation in order to become gender-responsive. These avenues could be coordinated with the ISO's overall Gender Action Plan. ISO standards have a default 3-year cycle of revisions, into which new gender-based recommendations can be incorporated. ISO standards can also be revised early if an urgent issue is identified.

## 3.2 Areas for further investigation

An important subject for additional research refers to ways to address potential gendered impacts in cybersecurity standards. These include gender-based violence facilitated by home devices connected to the

Internet[58] and the disproportionate effect of data breaches on men and women.[59] Although cybersecurity in technology supply chains has received extensive attention,[60] it is possible that cybersecurity standards around "clean" supply chains (i.e. those that do not introduce malicious code or raise the risk of malicious interference) also have indirect gendered impacts due to the participation of men and women in relevant occupations (e.g. in microchip factories).

Another important area for further investigation relates to the integration of gender-responsive cybersecurity standards into research and policy on basic Internet protocols. As part of wider efforts to address the human rights impacts of Internet protocols at the IETF,[61] several documents have suggested that a gender analysis of these protocols is necessary.[62] These debates over the "neutrality" of Internet protocols could be usefully applied to cybersecurity standards, as illustrations of how – and how not – to incorporate gender considerations into technical environments.

## 3.3 Recommendations

- International standards organizations, in cooperation with national standards bodies, should identify, and collect data on, the areas where cybersecurity standards have gender effects.
- Based on data collection and analysis, current cybersecurity standards should be revised in a gender-sensitive and gender-responsive manner.
- All proposed new cybersecurity standards should be subject to a gender impact assessment to ensure gender sensitivity and gender responsiveness. Practitioners should be given gender and cybersecurity training to support them in conducting these assessments.

- International standards organizations and national standards bodies should ensure that all working groups developing cybersecurity standards have gender and intersectional equality experts.
- International standards organizations and national standards bodies should ensure diverse gender representation in cybersecurity standard-making processes, in stakeholder consultations and within standards organizations.

# 4. Defence

How we think about defence – that is, what it means to defend and the common-sense actions we take to defend – is gendered. It reflects a series of norms associated with masculinity (e.g. protection, technical competence, autonomy, etc.) that derive from military understandings of national security.[63] This is often positive since it makes cybersecurity intelligible for a wide range of non-experts through the use of parallel concepts and language.

It can also, however, have negative effects. Many of the challenges associated with gender and cybersecurity defence derive from a mismatch between conventional understandings of national defence and cybersecurity, which is premised upon mitigating and managing, rather than eliminating, risks. Masculine norms and expectations that relate to using force to produce physical safety, for instance, may lead policy makers to downplay non-physical harms in cybersecurity.[64]

Masculine gender norms around vulnerability can make admitting error, seeking help or working cooperatively more difficult.[65] This can lead to reluctance to actively pursue cybersecurity defence or to be adequate transparent about failures to clients, employees or citizens. Such norms can also lead to the prioritization of some individuals and organizations – often those seen as socially prestigious or valuable for defence and protection (such as the State, the military or large corporations) – over others (such as civil society organizations and individuals, notably women and LGBTQ+[66] people).[67] A full gender perspective on cybersecurity defence recognizes that civil society and groups representing women and LGBTQ+ people have a need for, and a right to, cybersecurity defence – including the State resources (in terms of capacity-building, expertise and enforcement) needed to provide it.

More specifically, different elements of cybersecurity defence raise separate gender issues. Threats need to be monitored through the continuous evaluation and analysis of networks, infrastructure and devices for potential intrusions or deliberate disruption.[68] Following from this, at a basic level, what is considered to be a threat is gendered. Cybersecurity is typically concerned with military and corporate security (and thus threats relating to espionage and economic theft). A gendered understanding of cybersecurity threat, however, recognizes that those "traditional" threats, such as denial of service attacks on State services, have gendered outcomes.[69] It also recognizes that intimate partner violence, doxing, cyberstalking and the non-consensual dissemination of intimate images (i.e. "revenge porn") are also threats that can arise from the intrusion into or disruption of personal devices and networks.[70]

In terms of technical processes, insofar as threat monitoring relies on machine learning it is vulnerable to importing the gendered issues that typify the machine learning field, including gendered assumptions built into algorithms and biased data.[71] Even this largely automated process rests on human judgments about organizational priorities, allocation of resources and capacity building – all of which open the potential for the creation or intensification of inequalities. For instance, an automated email filter that identifies potentially harmful emails should flag romantic scams as well as phishing emails and financial scams.[72]

The processes of preparing for and responding to threats are also gendered. Threat simulations, for instance, such as the common practice of fake phishing emails, often involve gender stereotyping (e.g. a woman in an assistant role, a man as CEO).[73] There is a lack of gender-disaggregated data on phishing victims, which makes the gender consequences of phishing difficult to assess. But such an assessment is essential since, if

many cybersecurity breaches result from human error, policy makers need to have a variety of approaches to the "human" making the errors.

Bug bounty programmes, which are a spectrum of ways for "friendly" hackers to identify an organization's vulnerabilities and defence responses through digital, social or physical vectors, raise associated issues. As these contests are designed to be anonymous, only pseudonymic data (i.e. pertaining to hackers' aliases) is available on prolific bounty hunters and their payments. The consequences of this anonymity are unclear: it may make it easier for women and LGBTQ+ people to participate or it may exacerbate the gendered inequalities of cybersecurity and hacking culture more generally (see the case study below). Furthermore, the characterization of threats themselves, from the hooded hacker popular in media portrayals to code names and pictures used in cybersecurity technical reports, also often include gendered qualities and harmful stereotypes.[74]

Finally, attempts to protect organizations (and, to some extent, individuals) from the costs and harms arising from cybersecurity attacks, predominantly through cybersecurity insurance policies, should also be assessed for gender implications.[75] As with all insurance, it is important that threat assessments include gender analysis; that the criteria for being insurable can be met by women, men and non-binary people; and that pricing for organizations and individuals does not rely on gender stereotypes or produce discriminatory gender outcomes.[76]

### 4.1 Case study: talent and expertise

Talent and expertise is a widely recognized issue in the cybersecurity industry. Although the question of talent and expertise obviously pertains to all aspects of cybersecurity, we focus here on the practice of "defence" (i.e.

implementing security) since it is typically understood as cybersecurity's central activity.

Issues around talent and expertise are often expressed as a "gap" in cybersecurity expertise, meaning that the number of positions available is greater than the number of people qualified to fill them.[77] As demonstrated by research by organizations such as the Global Forum on Cyber Expertise, this talent gap is global, although pressures are expressed differently in different local contexts.[78] Many States have taken steps to incentivize people to join the cybersecurity industry and improve their level of skill once there. This is frequently complicated by competitive pressure between governments and the private sector, as government positions struggle to compete with private sector salaries.[79]

These issues with talent and expertise are exacerbated by gendered inequality, harms and visibility. Due to space constraints, this section discusses these dynamics quite generally. Understanding how and why gendered gaps, inequalities and harms operate in context, however, requires intersectional gender analysis that looks at how gender, race, sexuality, class, and rural or urban location, among other factors, interact to support the participation of some groups in cyber fields while marginalizing others.

A recent survey by the International Information System Security Certification Consortium indicated that 24 per cent of cybersecurity professionals worldwide are women.[80] The 2017 Global Information Security Workforce Study found that this lack of representation was accompanied by various forms of inequality, with 87 per cent of women reporting unconscious discrimination and 19 per cent overt discrimination.[81] This is a widely recognized problem, with many websites and social media accounts creating "women in cybersecurity" networks and events specifically for women.[82] Similar events, networks

and capacity-building initiatives also exist to support the equality, equity and participation of queer people in cybersecurity.[83] Following criticism of a lack of representation and visibility in cybersecurity conferences,[84] events such as the RSA Conference – a prestigious series of international information technology (IT) events – have sought to ensure gender parity in keynote speakers and to increase the participation of women overall.[85]

We split the gender issues for cybersecurity talent and expertise into three separate areas: the broader gender dynamics in science, technology, mathematics and engineering (STEM) professions; gender in computer science and coding; and gender in the cybersecurity industry specifically. We recognize that not all cybersecurity positions are STEM or "technical" positions; the prominence of these positions within cybersecurity reflects a gendered valuation of jobs understood as "masculine" above others. These positions are also, however, where gender disparities are most evident, and so we focus on these positions in this section.

### 4.1.1 Gender dynamics in STEM

Gender issues within STEM professions – again understood as a "gender gap" between men and women – are well-researched and typically understood in terms of pipeline and retention.[86] It should be noted that much of this research and policy follows a binary, often heteronormative understanding of gender; much more needs to be done to understand the experiences and support the equitable participation of non-binary and queer people within STEM and cybersecurity. The causes of the "gender gap" are complex and context specific. Generally, barriers to gender equality in STEM include (a) disparities in access to infrastructure and education; (b) individual- and family-level financial constraints and priorities; and (c) the persistence of sociocultural and institutional gender norms that

suggest STEM professions are predominantly for men.[87] In some contexts, such as Malaysia and the Middle East, women's participation in STEM education is considerable but is not translated into STEM careers.[88] In the United States of America and the United Kingdom, in contrast, girls remain less likely to be encouraged to pursue study of STEM subjects and less likely to regard themselves as holding STEM talent or expertise.[89]

Many of the policies aimed at increasing the participation of women in STEM can also be applied to the cybersecurity industry. These include greater incorporation of STEM skills into girls' education;[90] the promotion of STEM university programmes to girls and women;[91] actively recruiting women through campus visits and social media campaigns;[92] offering mentoring and continuing education to women and girls already employed within organizations; and altering human resources policies to prioritize hiring and retaining women (e.g. by requiring that at least one woman be interviewed for all open positions; by improving parental leave policies, etc.).[93] Disparities are often found in senior positions in STEM and technology start-ups and, given that cybersecurity is a young and fast-evolving field, the gendered dynamics of entrepreneurship are highly relevant.[94]

### 4.1.2 Gender in computer science and coding

Fields that centrally involve computers and "coding" (an unsatisfactorily generic term for a wide range of distinct skills) have well-documented gendered problems. Although, again, it differs across contexts, there is a global digital literacy gap[95] between women and girls and men and boys.[96] Worldwide, "327 million fewer women than men have a smartphone and can access the mobile Internet", while women are four times less likely than men to be IT professionals.[97]

It is worth remembering that early computing was relatively open to women and came to be seen as a masculine profession only as it rose in social prestige through its increasing importance to the economy.[98] Research has demonstrated that some online communities arranged around coding – including gaming and hacking – demonstrate a masculinist culture that emphasizes aggressive language and individuated approaches to problem-solving and technical mastery, while devaluing characteristics perceived to be associated with femininity, such as empathy and the expression of emotion.[99] These cultures can be explicitly misogynistic and homophobic, referring to women primarily as sex objects and to LGBTQ+ people in hateful and exclusionary terms.[100]

As these communities are often seen as a talent pool for cybersecurity expertise, there is a risk that cybersecurity recruitment will import anti-feminist and exclusionary norms (i.e. attitudes and practices that oppose and devalue gender equality and racial, ethnic and sexual inclusivity) into the workplace.[101] This makes work environments uncomfortable (or hostile) to those who do not conform.[102] The 2017 Global Information Security Workforce Survey found

## essentialism

Essentialism is an understanding of gender that assumes that humanity is divided into two biologically distinct sexes – male and female – and that these sexes determine the inherent behaviour and characteristics of men and women. It is often associated with perspectives that assume that all women (and all men) are the same and therefore have the same interests, needs and capacities. This can obscure important intersectional differences among women (and men and non-binary people) with respect to race, class, sexuality, caste and ability, among other things. A robust gender perspective recognizes that, although there are empirical patterns of difference between men and women, these patterns do not reflect essential characteristics and are therefore not inevitable.[107]

that 51 per cent of women in the field had experienced discrimination, compared to 15 per cent of men.[103] This primarily affects women and marginalized groups, but may also affect men who do not identify with such norms.[104] Workplaces that do not have an explicitly anti-feminist culture may still be organized and operated on the assumption that most workers are men and that values and practices associated with masculinity are neutral or "normal".[105] Although often without discriminatory or conscious intent, this perpetuates the gendered structure of cybersecurity expertise and thus influences hiring, opportunities for promotion and the ability to determine policy.

Where women do enter these fields, their contribution is often framed with reference to essentialist characteristics such as emotional and social skills. Although these are positive attributes, framing women's contributions predominantly in terms of, for example, empathy or caring solidifies gender stereotypes without necessarily increasing the value attributed to emotional, social and caring aspects of cyber expertise.[106]

A greater presence of women (and other members of marginalized groups) working in cybersecurity is believed to have two benefits. First, it can contribute to creative problem-solving and better policy governance and implementation through the introduction of diverse perspectives.[108] Second, it is believed that these perspectives will lead to a gender perspective in cybersecurity overall.[109] Research indicates that this can occur but that, without support, women and members of other minoritized groups may instead feel pressure to adapt to the workplace norm.[110] Tokenized incorporation of women and members of minoritized groups, without recognizing their contributions or in ways that reinforce stereotypes, do not contribute to meaningful participation or greater equality.[111]

### 4.1.3 Gender in the cybersecurity industry

Some gendered issues relate specifically to the cybersecurity industry. As the field of cybersecurity is growing in importance, influence and prestige, women's participation in cybersecurity is a matter of equality and equity in terms of opportunities for success, recognition and earning potential. Some working practices in cybersecurity, such as the shift requirements of Security Operation Centres, require further analysis to assess their gendered implications. Similarly, many cybersecurity certification programmes require intense sprints with long hours, which is an impractical work model for people (more likely to be women) with childcare responsibilities.[112]

More subtly, the cultivation of work environments, institutional cultures and management styles that are skeptical of traditional or conventional authority, although often praised as a characteristic of an innovative workforce, agile organization and dynamic socio-technological sector, can facilitate a narrow understanding of masculinity (and discrimination) akin to the wider fields above.[113] Addressing the "gender gap" in cybersecurity expertise therefore requires policies that promote the inclusion and participation of women and gender training to reduce harassment and discrimination and to support organizational and cultural shifts to value a variety of activities and capacities, including those usually more associated with femininity.[114]

## 4.2 Areas for further investigation

Many areas of gender and cyber expertise require additional research. The debates regarding STEM and digital "gender gaps" need to be contextualized (i.e. in specific countries, intergovernmental organizations, corporations etc.) and examined using intersectional gender analysis. There is a particular absence of data regarding the obstacles and opportunities

experienced in professional cybersecurity (and STEM education) by non-binary and LGBTQ+ people, as well as people from other minoritized (e.g. racial, ethnic, religious) backgrounds. Policies that aim to transform structural obstacles, rather than support individuals to succeed despite them, should be prioritized.

Greater attention should also be paid to understanding differences in private and public sector approaches to, and experiences of, gender and cyber expertise. Professional structures, incentives and hiring practices differ between the two sectors.[115] It is therefore important to know whether gender dynamics occur in the same way and to consider whether best practices might be shared between them. Correspondingly, we ought to ask if there is a difference in the technical literacy (and, indeed, gender equality commitments) of private and public experts. Similar research should be conducted comparing (in context) private sector uptake of gender equality policies in hiring, retention and professional development.

## 4.3 Recommendations

» International organizations, States and professional bodies should ensure that policies to promote gender equality and equity in cybersecurity are sensitive to local contexts and gender dynamics. States in particular should build on successful similar policies in STEM generally, including interventions that seek to change current educational systems rather than simply facilitating success within them.

» All public and private sector organizations should take active measures to counter anti-feminist and exclusionary workplace norms in cybersecurity and to create a safe and inclusive environment for all genders through mandatory gender training and meaningful leadership by senior management.

- Through incentives and regulation, States should encourage private sector uptake of gender equality policies in design, hiring and self-regulated professionalization.
- Policy makers at the State and international levels, as well as private sector practitioners, should apply a gender perspective to identify "default" (often male/masculine) assumptions in cybersecurity policies and practices, and revise them accordingly.
- All organizations, but particularly the private and educational sectors, should act to mitigate gender stereotypes in recruitment and professional practices by avoiding unjustified associations between women and "softer" cybersecurity skills.
- Educational organizations, professional and regulatory bodies, and employers should promote and support groups and networks for women, non-binary people and LGBTQ+ members of the cybersecurity professional community. States and academics should collect data on, and create policy based on, the experiences in the cybersecurity profession (and in STEM education) of LGBTQ+ and non-binary people, as well as people from other minoritized backgrounds.

# 5. Response

Incident response – organizational measures to handle network intrusions, attacks, data breaches and other malicious cyber acts – is characterized by a hierarchy of priorities. Studies have shown that the cybersecurity industry reports on and responds to certain victims (commercial organizations, governments) that are associated with "traditional" security and the activities of elite men disproportionately, and it has a blind spot for threats to civil society and human security (e.g. non-governmental organizations, educational institutions and individuals).[116] As schools, non-governmental organizations and individuals are more likely to be concerned with issues of social power, harms and equality, this prioritization has knock-on gender effects.

The composition, expected practices and working hours, and workplace culture of incident-response teams also require a gender analysis. There is some evidence that "tech support" teams, which are often the first line of response following a security incident, are predominantly staffed by men, compounding the association of technical expertise with masculinity.[117] The composition and culture of Computer Emergency Response Teams (CERTs or CSIRTs) is also a part of cybersecurity response. Research indicates that CERTs have distinct political strategies and characteristics, especially at the national and international levels, and it is possible that these characteristics include gendered dynamics.[118]

Information sharing – the process of trusted exchange of information about attacks and other security incidents, vulnerabilities, and cybersecurity practices – is also an essential part of responding to cybersecurity threats. The same masculine, national defence norms may also impede States and organizations from sharing information about cyberattacks and system vulnerabilities. Studies suggest that informal "trust communities" are the basis for much cybersecurity information sharing, rather than formal lines of communication between individuals with similar roles.[119]

The informality of these communities, and the consequent unconscious bias that this permits, means that they may have lower participation from women and minoritized groups, even when adjusted for overall proportions in the industry. Cybersecurity response can also demonstrate an unfortunate gendered dynamic of victim-blaming, wherein organizations or individuals with cybersecurity defence or identity-protection measures that are deemed to be "insufficient" are framed as "asking to be hacked", which shifts responsibility onto the party that has been harmed, rather than the one who committed harm.[120]

Cybersecurity insurance is also an important part of the response pillar. While not a substitute for the proper handling of cybersecurity incidents, compensation can help to recover damages directly related to a particular incident. Insurers have also been effective in shifting policyholders towards professionalized incident response.[121] However, corporate insurance policies are likely to perpetuate existing gender biases in the object of cybersecurity, by reflecting and reinforcing gendered hierarchies in the prioritization of cybersecurity targets. The developing market for individual cybersecurity insurance policies, on the other hand, may introduce new biases in definitions of cyber bullying or differing levels of compensation for personal items and identity cards following fraud or identity theft.[122] Finally, gender-disaggregated data is required on cybersecurity insurance claims and pay-outs to determine whether there are discriminatory practices or unequal outcomes.[123]

## 5.1 Case study: legal measures

States use various policy and legal tools to respond to malicious digital acts. These tools include naming and shaming, diplomatic and economic

sanctions, and criminal justice. Legal frameworks play a crucial role in enabling State responses, both to inter-State malicious acts and to crime. Although legal frameworks are relevant to all pillars of security – for example, they may mandate measures for cybersecurity preparedness[124] – law is central to the "response" pillar. It covers many aspects of cybersecurity response, from facilitating information sharing to protecting security researchers engaged in vulnerability testing and detection. Criminal legal responses also define, investigate, prosecute, and deter malicious acts and actors.

While international law and norms play a crucial role in maintaining peace and security, States are the primary actors in addressing cybersecurity incidents on their "territory", using domestic legal tools. Despite the current separation between United Nations processes dealing with international cybersecurity and with cybercrime, the criminal justice responses to malicious behaviour in cyberspace and international cybersecurity are obviously interconnected.

In this regard, the report of the 2015 United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security includes pertinent recommendations. It recommends as a specific confidence-building measure that States should consider voluntary agreements to "Cooperate, in a manner consistent with national and international law, with requests from other States in investigating [information and communications technology (ICT)]-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory".[125] It also established a norm that calls for cooperation and assistance in mitigation of malicious ICT activity aimed at critical infrastructure.[126]

Legal responses are also crucial in deterring malicious actors and holding them accountable. Even perpetrators backed by a State should be brought to justice; avoiding impunity is essential to address any malicious activity in cyberspace, be it crime or acts of adversaries.[127] Given the problem of attribution and the lack of actual use of international law in response to cyberoperations,[128] many States have charged actors connected to the foreign adversaries under national criminal legislation.[129]

Based on States' use of their domestic criminal law to respond to adversaries' malicious acts,[130] we consider criminal legal responses to be crucial to cybersecurity. This goes beyond the issue of so-called "cybercrime". The criminal legal procedures for the investigation of computer crimes can be used for the investigation of virtually any criminal act. In many countries, law enforcement and intelligence services share information and tools for the investigation of cybersecurity incidents.

Existing research has demonstrated that incidents falling under wider definitions of cybersecurity than that adopted here have a gendered impact.[131] This is obvious in the case of online-based harassment and violence, wherein women and LGBTQ+ people are disproportionately targeted.[132] Moreover, various gender-based concerns have also been identified in relation to Internet shutdowns and data breaches. Online violent extremism and online sex trafficking, which target men and boys as well as women and girls, also falls into this category.[133] Unfortunately, legal responses to cybersecurity incidents have not addressed these gendered impacts in a systematic way, thus exacerbating the problem that the law generally furthers the "articulation of gendered inequalities". [134]

Legal frameworks typically consider only the most immediately obvious aspects of gender and cybersecurity, such as harassment and violence directly targeted at, or committed by, identifiable people. Even then,

gender is not always incorporated in equitable ways. Gender-related issues hamper access to justice and courts, ranging from rigid expectations as to "appropriate" behaviour for men and women; differential access to the material resources and social capital required to pursue a case; bias relating to the relative credibility of men and women (particularly LGBTQ+ people); and differential resources committed to investigating and persecuting crimes that are typically experienced by men in comparison to those experienced by women (particularly minoritized or trans women) and non-binary people.[135] Essentialist assumptions that posit women as victims[136] and men as perpetrators contribute to processes of (re)victimization,[137] traumatization and – often for men, boys and marginalized women – over-incarceration.[138]

These dynamics can be exacerbated in the cyber domain. Crimes are often new or ill-defined,[139] leaving space for gender bias and essentialist assumptions to enter investigations and prosecution.[140] It is increasingly common for abusers to use "stalkerware" to monitor a victim, yet a recent study of United States and Canadian law revealed that manufacturers and users are rarely prosecuted for malicious technology use.[141]

Cyber law enforcement remains a field primarily staffed by men, suffers from a lack of trained judges and is characterized by masculine gender norms.[142] It is common in criminal investigations, for instance, to seize victims' devices as evidence (which may pose a personal security risk) and to download all images, violating victims' privacy and potentially undermining their credibility in cases of sexual assault or harassment.[143] If victims do not wish to share their personal data, authorities have in some instances declined to prosecute.[144] The growing use of AI in cybersecurity investigations and criminal justice makes victims, offenders and the entire system of law enforcement vulnerable to both gender and racial bias, amplifying existing gender-related issues and inequalities.[145]

Current legal frameworks for cyber incident investigations, especially those involving intelligence services and law enforcement agencies accessing data or ordering electronic surveillance with the use of remote forensic software, do not take into account the gendered impact of these intrusive tools. Relatedly, legal approaches to malicious cyber actors may reflect masculinist norms of law enforcement more broadly, particularly those that suggest punitive and aggressive counter-responses to be the best, and perhaps only, option for response.[146]

Gender is central to determining what a malicious act is – that is, identifying an offence and determining the appropriate response. While in some cases this leads to legislation about gender directly, such as the criminalization of certain forms of gendered and sexualized online harassment (e.g. hacking to acquire and post intimate photos without consent, sometimes to "sextort" additional sexual content),[147] a gender perspective is broader. It involves, in other words, systematic gender analysis of issues that do not seem to be immediately "about" women and girls (or men and boys). For example, legal responses to leaks of private information or hacking of medical records should consider the gendered impact of these incidents. In addition to potentially exposing the private medical information of all involved,[148]

## gender mainstreaming

Gender mainstreaming "is the process of assessing the implications for girls and boys and men and women of any planned action, including legislation, policies and programmes".[154] It is the United Nation system's primary strategy for accelerating progress on gender equality, by ensuring that the distinct perspectives and needs of women and girls and of men and boys are incorporated into all policy processes, to ensure inclusion and avoid the perpetuation of inequality.[155]

people with the ability to become pregnant may be particularly affected by the publication of their reproductive history,[149] while LGBTQ+ people's lives, livelihoods and well-being may be endangered through publication, and involuntary "outing", of their identities.[150]

Legal frameworks that respond to malicious acts in cyberspace are frequently rushed through in an alarmist, rather than empowering, manner. This results in State control and privacy violations, harming or re-victimizing those whom they are trying to protect.[151] For example, laws intended to protect women or vulnerable groups from online-based violence can be paternalistic, creating more possibilities for control, dominance and gender-related privacy infringement through implementation.[152]

All these policy changes require support and action by national legislative bodies as the primary actors responsible for drafting (and gender mainstreaming) cybersecurity legislation.[153] Therefore, it is important to facilitate an open and participatory legislative (and oversight) process, involving all stakeholders, especially civil society, women's rights groups and LGBTQ+ rights organizations in the discussion.

## 5.2 Areas for further investigation

We need a better understanding of the linkages between, on the one hand, norms related to responsible State behaviour and, on the other, national criminal justice responses to cyber threats and malicious acts in cyberspace. States increasingly resort to criminal justice for attribution, investigation and prosecution of the acts committed by adversaries, connecting cybersecurity with the complex gender dynamics of national laws and national criminal justice systems. While this does not mean that

separate United Nations processes on international cybersecurity and cybercrime should necessarily be brought together, the link between the two should be acknowledged and further researched to avoid isolating efforts to mainstream gender into cybersecurity.

Legal responses to malicious acts in cyberspace bring our cyber-centric approach to cybersecurity back into contact with human-centric approaches through laws regarding gender-based cyber violence, domestic abuse and harassment legislation. Effectively using the law to address cybersecurity thus requires considering the gender impact of all laws tackling cyber threats, from threats to integrity, confidentiality and availability of data in computer systems to harms to individuals.

Further research is required to assess whether this disparity results in different experiences of "tech support" by men, women and non-binary people. This work should also investigate whether the gender identity of the cybersecurity technical community informs people's willingness to report cybersecurity issues perceived as personal (e.g. revenge porn, romance scams, identity theft).

## 5.3 Recommendations

» National legislative bodies, in consultation with a wide range of stakeholders, including civil society and private industry, should identify the gender impact of (a) the cybersecurity incidents that law seeks to address, (b) the law itself and (c) its implementation.

» States, in consultation with wider stakeholders, should collect gender- and equality-disaggregated data to analyse the impact of existing legal responses, and revise laws accordingly.

- States, in cooperation with civil society and business, should create and implement a clear list of indicators to monitor the gender impact of legal responses to cybersecurity threats.
- States, in consultation with other stakeholders, should identify gender obstacles in accessing justice (i.e. law enforcement and the court system) and should work towards removing these obstacles. Training for police, prosecutors and judges is essential.
- International and regional organizations, States, and legislative bodies should further work on promoting gender-sensitive parliaments. Gender concerns should be a regular component of legislative committee oversight of cybersecurity law and practice.
- Legislation addressing gender and sexual equality (and risks and discrimination), such as intimate partner violence laws, should incorporate attention to digital technologies.[156] This should be supplemented by identifying the role and responsibilities of the private sector in implementation of gender-responsive legal frameworks and changes in the structure of digital interaction.
- Legal responses should recognize the limitations of criminal justice. Although criminal accountability is an important legal tool, it should not be the sole solution, particularly in instances where norm creation, restorative justice and diversion would be more appropriate or effective in addressing harms and preventing future incidents.[157]

# 6. Conclusions

This report adopts a gender approach to cybersecurity, proposing a new framework to help policy makers and practitioners to think through the gendered implications of cybersecurity design, defence and response. This three-pillar framework addresses the common misperception that the technical or technological aspects of cybersecurity are gender-neutral, and therefore gender-blind.

This analysis identifies key areas where cybersecurity practices require gender analysis or other gender policy interventions. The three-pillar approach, although simplified and schematic, enables a clear analytical delineation of different gender dynamics. In practice, there is extensive overlap and interaction between the pillars, and so improvements in one would lead to improvements in others.

The systematic analysis is supplemented by three in-depth case studies, examining cybersecurity standards, talent and expertise, and legal responses. These case studies explore the extent of existing research and policy on these three issues, emphasizing where research has already indicated gendered inequalities or other harmful effects, and pointing to areas for further research and policy interventions to counter such harms.

Each of the case studies leads to several recommendations to be implemented by States in conjunction with other stakeholders, including academia, civil society organizations, international and regional institutions, and

companies. We also make the overarching recommendation for the development and implementation of gender and cybersecurity training across all organizations and sectors of the field. This is an essential prerequisite for further improving gender equality and equity within the sector, as well as developing substantive expertise in gender analysis as a professional skill.

The overall objective of this research is to ensure that cybersecurity improves the security of people of all gender identities and expressions, as well as international peace and security. The ultimate conclusion is that these two levels of security cannot be separated.

# Endnotes

1. Non-binary is used here as a broad term to refer to gender identities that do not align with the gender binary (i.e. men/masculinity and women/femininity). This includes agender, genderfluid and genderqueer identities, as well as the many contextually specific non-binary gender identities that exist in societies around the world. The term, therefore, should be read broadly, rather than as implying a singular, monolithic third option. Non-binary is not a synonym for trans, which generally refers to people whose gender identity does not sit comfortably with the sex they were assigned at birth, many of whom identify as men or women. For more on this topic, see United Nations Free & Equal, "Definitions", https://www.unfe.org/definitions/; and Stonewall, "Glossary of Terms", https://www.stonewall.org.uk/help-advice/faqs-and-glossary/glossary-terms#n.

2. Due to space constraints and a relative lack of existing research, this report primarily examines the differential experiences and opportunities of predominantly cisgender men and women in cybersecurity. Robust gender analysis, however, should be intersectional: attentive to the ways in which multiple forms of social power, relating to class, race, coloniality, nationality, ability, ethnicity, caste, sexual orientation, age and gender expression etc. work alongside gender to produce patterns of marginalization and exclusion. Additional research into these intersections, conducted in both the Global North and Global South, is essential. K. Crenshaw, "Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Colour", Stanford Law Review, vol. 43, no. 6, July 1991, pp. 1241–1299, https://doi.org/10.2307/1229039; and Combahee River Collective, "A Black Feminist Statement", Women's Studies Quarterly, vol. 42, no. 3/4, fall/winter 2014, pp. 271–280, https://www.jstor.org/stable/24365010, pp. 210–218.

3. UN Women, "Concepts and definitions", https://www.un.org/womenwatch/osagi/conceptsandefinitions.htm; UNICEF Regional Office for South Asia, Gender Equality: Glossary of Terms and Concepts, November 2017, https://www.unicef.org/rosa/media/1761/file/Gender%20glossary%20of%20terms%20and%20concepts%20.pdf; and Canadian Institutes of Health Research, "What is gender? What is sex?", 28 April 2020, https://cihr-irsc.gc.ca/e/48642.html.

4. E.g. statements submitted to the OEWG by States and non-State stakeholders, United Nations, Office for Disarmament Affairs, "Open-ended Working Group", https://www.un.org/disarmament/open-ended-working-group/; and "Informal Intersessional Consultative

Meeting of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Chair's Summary", 2–4 December 2019, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/200128-OEWG-Chairs-letter-on-the-summary-report-of-the-informal-intersessional-consultative-meeting-from-2-4-December-2019.pdf. I. Nakamitsu, Opening Address by to the Group of Governmental Experts on Advancing responsible State Behaviour in Cyberspace in the Context of International Security, 9 December 2019, https://www.un.org/disarmament/wp-content/uploads/2019/12/HR-addresses-GGE-on-advancing-responsible-State-behaviour-in-cyberspace-.pdf.

5. For detailed information on national statements highlighting the importance of gender mainstreaming in the OEWG process, see Cyber Peace & Security Monitor, vol. 1 no. 7, 18 February 2020, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.7.pdf. See also "Canada's Proposal for the Report of the 2019–20 United Nations Open-Ended Working Group on 'Developments in the Field of Information and Telecommunications in the Context of International Security'", Working paper submitted by Canada, https://www.un.org/disarmament/wp-content/uploads/2019/09/canadian-position-paper-oewg-en.pdf.

6. On the distinction between gender identity and gender expression, see Ontario Human Rights Commission (OHRC), Policy on Preventing Discrimination Because of Gender Identity and Gender Expression, 14 April 2014, Appendix B, "Glossary for Understanding Gender Identity and Expression", http://www.ohrc.on.ca/en/policy-preventing-discrimination-because-gender-identity-and-gender-expression/appendix-b-glossary-understanding-gender-identity-and-expression.

7. UNICEF Regional Office for South Asia, Gender Equality: Glossary of Terms and Concepts, November 2017, https://www.unicef.org/rosa/media/1761/file/Gender%20glossary%20of%20terms%20and%20concepts%20.pdf. See also UN Women, "Concepts and definitions", https://www.un.org/womenwatch/osagi/conceptsandefinitions.htm.

8. J. Shires, "Family Resemblance or Family Argument? Three Perspectives of Cybersecurity and Their Interaction", St Anthony's International Review, vol. 14, no. 3, 2019, pp. 18–36, https://www.ingentaconnect.com/content/stair/stair/2019/00000015/00000001/art00003.

9. E.g. 71% of incidents are attributed to financially motivated crime and only 25% to espionage by Verizon, Verizon Data Breach Investigations Report 2019, 2019, https://enterprise.verizon.com/en-nl/resources/reports/dbir/2019/summary-of-findings/

10. E.g. through automated malware generation or botnet control.

11. J. Shires, "Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States", War on the Rocks, 12 October 2018. https://perma.cc/L4CL-2B8A. See also P. Cornish, "Governing Cyberspace through Constructive Ambiguity", Survival, vol. 57, no. 3,

May 2015, pp. 153–76, https://doi.org/10.1080/00396338.2015.1046230; M. Raymond and L. DeNardis, "Multistakeholderism: Anatomy of an Inchoate Global Institution", International Theory, vol. 7, no. 3, November 2015, pp. 572–616, https://doi.org/10.1017/S1752971915000081; and A. Grigsby, "The End of Cyber Norms", Survival, vol. 59, no. 6, November 2017, pp. 109–122, https://doi.org/10.1080/00396338.2017.1399730.

12. See e.g. National Coordinator for Security and Counterterrorism, "Cyber Security Assessment Netherlands", Ministry of Justice and Security, 2019, https://english.ncsc.nl/topics/cybersecurity-assessment-netherlands. The US Senate Armed Services Committee held a cybersecurity subcommittee session on leaks in April 2017, leading to descriptions of Russian leaks as a cybersecurity issue in many subsequent publications. "Like-minded" states have always included some content controls under terrorism legislation, but the definition of terrorism is another thorny issue. Another way of putting this point is that our definition of cybersecurity uses a narrow version of integrity in the traditional "Confidentiality, Integrity, Availability" (CIA) triad in computer and information security.

13. Hack-and-leak operations involve obtaining sensitive data through cyber intrusion (hack) and distributing that data in the public domain (leak). J. Shires, "Hack-and-Leak Operations: Intrusion and Influence in the Gulf", Journal of Cyber Policy, vol. 4, no. 2, 2019, pp. 235–56, https://doi.org/10.1080/23738871.2019.1636108; and J. Shires, "The Simulation of Scandal: Hack-and-Leak Operations, the Gulf States, and U.S. Politics", Texas National Security Review, vol. 3, no. 4, fall 2020, https://tnsr.org/2020/08/the-simulation-of-scandal-hack-and-leak-operations-the-gulf-states-and-u-s-politics/.

14. See chapter 5 of this report.

15. G. Wellner and T. Rothman, "Feminist AI: Can We Expect Our AI Systems to Become Feminist?", Philosophy & Technology, vol. 33, no. 2, June 2020, pp. 191–205, https://doi.org/10.1007/s13347-019-00352-z.

16. T.L. Wagner and A. Blewer, "'The Word Real Is No Longer Real': Deepfakes, Gender, and the Challenges of AI-Altered Video", Open Information Science, vol. 3, no. 1, 2019, pp. 32-46, https://doi.org/10.1515/opis-2019-0003; and S. Maddocks, "'A Deepfake Porn Plot Intended to Silence Me': Exploring Continuities between Pornographic and 'Political' Deep Fakes", Porn Studies, vol. 7, no. 4, 2020, pp. 415–423, https://doi.org/10.1080/23268743.2020.1757499.

17. A. Marwick and R. Lewis, Media Manipulation and Disinformation Online, Data & Society Research Institute, 2017, https://www.datasociety.net/pubs/oh/DataAndSociety_MediaManipulationAndDisinformationOnline.pdf.

18. These impacts include women in public political life, cyberbullying for children and young people. K. Blake, M. Godwin and S. Whyte, "'I Sexually Identify as an Attack Helicopter': Incels, Trolls, and Non-Binary Gender Politics Online", First Monday, vol. 25, no. 9, 2020, https://doi.

org/10.5210/fm.v25i9.10601; K. Hendricks, P. Tsibolane and J.-P. van Belle, "Cyber-Harassment Victimization Among South African LGBTQIA+ Youth", In Conference on e-Business, e-Services and e-Society, Springer, 2020, pp. 135–146, https://doi.org/10.1007/978-3-030-45002-1_12; and S. Yao, "Gender Violence Online", In Handbook on Gender and Violence, Edward Elgar, 2019, https://doi.org/10.4337/9781788114691.00022.

19. J. Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity", St Anthony's International Review, vol. 15, no. 1, May 2019, pp. 83–100, https://papers.ssrn.com/abstract=3429851.

20. The main alternative approach to this "cyber-centric" framework is what might be termed a "human-centric" approach, which is more common to gender analysis. For an example of such an approach, see the work highlighting the differential impact of certain types of cyberincident according to gender (e.g. internet shutdowns, data breaches, etc.) in D. Brown and A. Pytlak, Why Gender Matters in International Cyber Security, Women's International League for Peace and Freedom (WILPF) and the Association for Progressive Communications (APC), April 2020, https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf. By highlighting technical expertise in this way, we do not imply that other forms (such as policy expertise) are not relevant to cybersecurity; on the contrary, we examine their gendered assumptions in subsequent chapters of this report.

21. L. Sjoberg, "Gender, Structure, and War: What Waltz Couldn't See", International Theory, vol. 4, no. 1, pp. 1–38, https://doi.org/10.1017/S175297191100025X; L. Wilcox, "Gendering the Cult of the Offensive", Security Studies, vol. 18, no. 2, 2009, pp. 214–240, https://doi.org/10.1080/09636410902900152; and J. Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity", St Anthony's International Review, vol. 15, no. 1, May 2019, pp. 83–100, https://papers.ssrn.com/abstract=3429851.

22. E.g. US National Institute of Science and Technology (NIST), "Cybersecurity Framework", https://www.nist.gov/cyberframework.

23. The "kill chain" is a model for representing the many steps involved in a cyberattack (and therefore the many opportunities for cybersecurity defence to disrupt the attack). E.M. Hutchins, M.J. Cloppert and R.M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Lockheed Martin Corporation, 2010, https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

24. Proposed by the fourth United Nations Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, General Assembly, A/70/174, 22 July 2015, http://undocs.org/A/70/174.

25. L.M. Tanczer, "Post, Gender, Internet?", In C. Landler, P. Parccek, and M.C. Kettemann, (eds.), Netzpolitik in Österreich. Internet. Macht. Menschenrechte [Network Policy in Austria. Internet. Power. Human Rights], Internet & Gesellschaft Co:llaboratory AT, June 2013, pp. 53–69, http://publikationen.collaboratory.co.at/mri/2013/08/09/post-gender-internet/; and J. Wajcman, "From Women and Technology to Gendered Technoscience", Information, Communication & Society, 2007, vol 10, no. 3, pp. 287–298, https://doi.org/10.1080/13691180701409770. See also UNESCO and EQUALS Skills Coalition, "I'd Blush If I Could: Closing Gender Divides in Digital Skills through Education", United Nations, 2019, https://en.unesco.org/Id-blush-if-I-could; and C.C. Perez, Invisible Women: Data Bias in a World Designed for Men, Harry N. Abrams, 2019.

26. These extensive bodies of research dovetail with an approach termed "human-centred computing", more directly relevant to cybersecurity.

27. A. Robertson, "Building for Virtual Reality? Don't Forget about Women", The Verge, 11 January 2016, https://www.theverge.com/2016/1/11/10749932/vr-hardware-needs-to-fit-women-too. See also Y. Strengers and J. Kennedy, The Smart Wife: Why Siri, Alexa, and Other Smart Home Devices Need a Feminist Reboot, MIT Press, 2020, https://doi.org/10.7551/mitpress/12482.001.0001.

28. Ibid; and UNESCO and EQUALS Skills Coalition, "I'd Blush If I Could: Closing Gender Divides in Digital Skills through Education", United Nations, 2019, https://en.unesco.org/Id-blush-if-I-could.

29. Mrs Smith, "Can We Avoid Marginalizing Women with the Internet of Things?", Medium, 30 December 2015, https://medium.com/@hauspa/can-we-avoid-marginalizing-women-with-the-iot-42ecbdf9f67a.

30. C. Beaudry and V. Larivière, "Which Gender Gap? Factors Affecting Researchers' Scientific Impact in Science and Medicine", Research Policy, vol. 45, no. 9, November 2016, pp. 1790–1817, https://doi.org/10.1016/j.respol.2016.05.009; and L. Holman, D. Stuart-Fox and C.E. Hauser, "The Gender Gap in Science: How Long Until Women are Equally Represented?", PLoS Biology, vol. 16, no. 4, 2018, e2004956, https://doi.org/10.1371/journal.pbio.2004956.

31. J. Slupska and L.M. Tanczer, "Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things", In J. Bailey, A. Flynn and N. Henry (eds.), The Emerald International Handbook of Technology-Facilitated Violence and Abuse, forthcoming 2021. See also S. Parkin et al., "Usability Analysis of Shared Device Ecosystem Security: Informing Support for Survivors of IoT-Facilitated Tech-Abuse", Proceedings of the New Security Paradigms Workshop, September 2019, pp. 1–15, https://doi.org/10.1145/3368860.3368861.

32. See e.g. the resources at Refuge, "Tech abuse and tech safety resources", https://www.refuge.org.uk/our-work/forms-of-violence-and-abuse/tech-abuse-2/resources/.

33. Gendered threat models may also be present at State levels, such as in vulnerability equities processes. See S. Herpig and A. Schwartz, "The Future of Vulnerabilities Equities Processes Around the World", Lawfare, 4 January 2019, https://perma.cc/6U3P-38JA.

34. D. Woodlock, "The Abuse of Technology in Domestic Violence and Stalking", Violence Against Women, vol. 23, no. 5, 2017, pp. 584–602, https://doi.org/10.1177/1077801216646277; C. Essert, "Addressing Imperfect Solutions to Technology-Facilitated Domestic Violence", Women's Rights Law Reporter, vol. 41, 2019, p. 117; D. Woodlock et al., "Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control", Australian Social Work, vol 73, no. 3, 2020, pp. 368–380; and K. Levy and B. Schneier, "Privacy Threats in Intimate Relationships", Journal of Cybersecurity, vol. 6, no. 1, 2020, tyaa006, https://doi.org/10.1093/cybsec/tyaa006.

35. E.g. A. Malik, K. Hiekkanen and M. Nieminen, "Privacy and Trust in Facebook Photo Sharing: Age and Gender Differences", Program, vol. 50, no. 4 (January 2016), pp. 462–480, https://doi.org/10.1108/PROG-02-2016-0012; and S. Tifferet, "Gender Differences in Privacy Tendencies on Social Network Sites: A Meta-Analysis", Computers in Human Behavior, vol. 93, April 2019, pp. 1–12, https://doi.org/10.1016/j.chb.2018.11.046. For an older, contrary, conclusion, see d. boyd and E. Hargittai, "View of Facebook Privacy Settings: Who Cares?", First Monday, vol. 15, no. 8, 2010, https://firstmonday.org/article/view/3086/2589.

36. B.A. Harris and D. Woodlock, "Digital Coercive Control: Insights from Two Landmark Domestic Violence Studies", British Journal of Criminology, vol. 59, no. 3, 2019, pp. 530–550, https://doi.org/10.1093/bjc/azy052.

37. Ibid.

38. It should be noted that children's rights to privacy, expression and safety (and the ways these might clash with parental desires) often do not – though they should – figure highly into discussions of cyberethics, cybersecurity and cybergovernance. For an overview of these complexities, see S. Livingstone and B. O'Neill, "Children's Rights Online: Challenges, Dilemmas and Emerging Directions", In S. van der Hof, B. van den Berg and B. Schermer (eds.), Minding Minors Wandering the Web: Regulating Online Child Safety, TMC Asser Press, 2014, pp. 19–38, https://doi.org/10.1007/978-94-6265-005-3_2.

39. C. Parsons et al., "The Predator in your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry", Citizen Lab, 2019, https://citizenlab.ca/docs/stalkerware-holistic.pdf.

40. C. Cimpanu, "Google Bans Stalkerware Ads", ZDNet, 9 July 2020, https://www.zdnet.com/article/google-bans-stalkerware-ads/.

41. ISO/IEC Directives, Part 2, "Principles and Rules for the Structure and Drafting of ISO and IEC Documents", 8th edn., 2018, https://www.iso.org/sites/directives/current/part2/

index.xhtml#_idTextAnchor007, Section 3.1.2. The ISO definition adds that a standard must be "established by consensus and approved by a recognized body". See also the World Trade Organization (WTO) definition: "standards set out specific characteristics of a product – such as its size, shape, design, functions and performance, or the way it is labelled or packaged", as well as specific process and production methods for that product. World Trade Organization, "Technical Information on Technical Barriers to Trade", https://www.wto.org/english/tratop_e/tbt_e/tbt_info_e.htm.

42. Regulations can reference standards, but national standards bodies are usually separate to regulators (as is WTO best practice). Ibid.

43. Link to the full roadmap of cybersecurity standards and organizations developing them: International Telecommunication Union (ITU), "Security Standards Under Development", ICT Security Standards Roadmap, https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/ict-part03.aspx.

44. United Nations Economic Commission for Europe, "Gender Responsive Standards", 2019, https://www.unece.org/fileadmin/DAM/trade/Publications/ECE_TRADE_445E.pdf, p. 1.

45. International Telecommunication Union (ITU), "ITU Women in Standardization Expert Group (WISE)", https://www.itu.int/en/ITU-T/wise/Pages/default.aspx.

46. The requirement that cybersecurity capacity-building be gender-sensitive, inclusive and non-discriminatory aligns with broader United Nations and Member State commitments to gender equality. These are formally expressed in the Convention on the Elimination of All Forms of Discrimination Against Women and reflected in the Millennium and Sustainable Development Goals (particularly SDG 5). UNICEF Regional Office for South Asia, Gender Equality: Glossary of Terms and Concepts, November 2017, https://www.unicef.org/rosa/media/1761/file/Gender%20glossary%20of%20terms%20and%20concepts%20.pdf.

47. United Nations Economic Commission for Europe, "Gender Responsive Standards Declaration", https://www.unece.org/tradewelcome/tradewp6/tradewp6thematicareas/gender-responsive-standards-initiative/gender-responsive-standards-declaration.html.

48. United Nations Economic Commission for Europe, "Gender Responsive Standards", 2019, https://www.unece.org/fileadmin/DAM/trade/Publications/ECE_TRADE_445E.pdf, pp. 8–9. For a wide range of examples see also C.C. Perez, Invisible Women: Data Bias in a World Designed for Men, Harry N. Abrams, 2019.

49. E.g. S. Mohan, "The Gendered Impact of Standards", Presentation, International Centre for Trade and Sustainable Development, 14 November 2018, http://www.unece.org/fileadmin/DAM/trade/wp6/documents/2018/PPTs/Sarah_Mohan_Gendered_Impact_of_Standards.pdf.

50. European Institute for Gender Equality, "Gender analysis", https://eige.europa.eu/gender-mainstreaming/methods-tools/gender-analysis.

51. Similar standards exist for certain sectors, e.g. PCI-DSS is widely considered the ISO 27001 equivalent for the financial sector.

52. IT Governance, "ISO 27000 Series of Standards", June 2020, https://www.itgovernance.co.uk/iso27000-family.

53. We consider both the ISO-wide Gender Action Plan and the work of the committee managing the 27000 series (ISO/IEC JTC1/SC 27) since these are separate initiatives.

54. This is a very recent development. Interviewees suggested that the exact format of this data, and its distribution when collected, has not yet been decided.

55. Thanks to Christina Runnegar for this point.

56. The implication is twofold: first, that the activity described using the term is seen as less important because of its lower status; and second, that the activity is assigned in a gendered way, passing this lower status on to those doing the work. For multiple examples of this process in action, see M. Hicks, M., Programmed Inequality: How Britain Discarded Women Technologists and Lost Its Edge in Computing, MIT Press, 2017.

57. Information obtained during interviews with stakeholders. The authors would like to thank Noelia Garcia Nebra and Dr. Edward Humphreys for their kind help with collection of relevant information and for useful insights into the gender-related ISO efforts. For a discussion of the gendered language that frames cybersecurity "common sense", see A. Lee, "It Starts with Words: Unconscious Bias in Gender, Race, and Class in Tech Terminology", 19 August 2020, https://www.localizationlab.org/blog/2020/8/19/it-starts-with-words-unconscious-bias-in-gender-race-and-class-in-tech-terminology.

58. L. Tanczer, "The Rise of the Internet of Things and Implications for Technology-Facilitated Abuse", University College London, November 2018, https://www.ucl.ac.uk/steapp/sites/steapp/files/giot-report.pdf.

59. As outlined in D. Brown and A. Pytlak, Why Gender Matters in International Cyber Security, Women's International League for Peace and Freedom (WILPF) and the Association for Progressive Communications (APC), April 2020, https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf.

60. T. Herr, Breaking Trust: Shades of Crisis Across an Insecure Software Supply Chain, Atlantic Council, July 2020, https://www.atlanticcouncil.org/programs/scowcroft-center-for-strategy-and-security/cyber-statecraft-initiative/breaking-trust/.

61. C. Cath and L. Floridi, "The Design of the Internet's Architecture by the Internet Engineering Task Force (IETF) and Human Rights", Science and Engineering Ethics, vol. 23, no. 2, April 2017, pp. 449–468, https://doi.org/10.1007/s11948-016-9793-y.

62. Internet Engineering Task Force (IETF), "Feminism and Protocols", 11 March 2019, https://tools.ietf.org/id/draft-guerra-feminism-00.html.

63. I.M. Young, "The Logic of Masculinist Protection: Reflections on the Current Security State", Signs: Journal of Women in Culture and Society, vol. 29, no. 1, 2003, pp. 1–25, https://doi.org/10.1086/375708; and F.J. Barrett, "The Organizational Construction of Hegemonic Masculinity: The Case of the US Navy", Gender, Work & Organization, vol. 3, no. 3, 1996, pp. 129–142, https://doi.org/10.1111/j.1468-0432.1996.tb00054.x.

64. See the research project F. J. Egloff and J. Shires, "Political Violence in Cyberspace", ETH Zürich, https://css.ethz.ch/en/research/research-projects/political-violence-in-cyberspace.html.

65. R. O'Brien, K. Hunt and G. Hart, "'It's Caveman Stuff, But That Is to a Certain Extent How Guys Still Operate': Men's Accounts of Masculinity and Help Seeking", Social Science & Medicine, vol. 61, no. 3, August 2005, pp. 503–516, https://doi.org/10.1016/j.socscimed.2004.12.008; and J.L. Berdahl et al., "Work as a Masculinity Contest", Journal of Social Issues, vol. 74, no. 3, September 2018, pp. 422–448, https://doi.org/10.1111/josi.12289.

66. LGBTQ+ refers specifically to lesbian, gay, bisexual, transgender and queer people, but the + signifies its broad inclusion of people of diverse, and often marginalized, gender identities, gender expressions and sexual orientations (which are not synonymous).

67. C. Enloe, Bananas, Beaches and Bases: Making Feminist Sense of International Politics, University of California Press, 2014, https://www.jstor.org/stable/10.1525/j.ctt6wqbn6; and L. Maschmeyer, R.J. Deibert and J. R. Lindsay, "A Tale of Two Cybers – How Threat Reporting by Cybersecurity Firms Systematically Underrepresents Threats to Civil Society", Journal of Information Technology & Politics, 2020, https://doi.org/10.1080/19331681.2020.1776658.

68. Threat monitoring can range in scale from fraud and individual identity theft to large-scale corporate cyberespionage.

69. D. Brown and A. Pytlak, Why Gender Matters in International Cyber Security, Women's International League for Peace and Freedom (WILPF) and the Association for Progressive Communications (APC), April 2020, https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf.

70. E.g. J. Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity", St Anthony's International Review, vol. 15, no. 1, May 2019, pp. 83–100, https://papers.ssrn.com/abstract=3429851.

71. S. Leavy, "Gender Bias in Artificial Intelligence: The Need for Diversity and Gender Theory in Machine Learning", In Proceedings of the First International Workshop on Gender Equality in Software Engineering, May 2018, pp. 14–16, https://doi.org/10.1145/3195570.3195580.

72. For more on romantic scams, see T. Yen and M. Jakobsson, "Case Study: Romance Scams", In M. Jakobsson (ed.), Understanding Social Engineering Based Scams, 2016, pp. 103–113, http://doi.org/10.1007/978-1-4939-6457-4_10; and A. Rege, "What's Love Got to Do with It? Exploring Online Dating Scams and Identity Fraud", International Journal of Cyber Criminology, vol. 3, no. 2, 2009, https://www.cybercrimejournal.com/aunshulregedec2009.htm.

73. This is especially the case for so-called "whaling" attacks, which target senior or powerful individuals.

74. J. Shires, "Cyber-Noir: Cybersecurity and Popular Culture", Contemporary Security Policy, vol. 41, no. 1, 2020, pp. 82–107, https://doi.org/10.1080/13523260.2019.1670006. For examples of harmful gendering of technologies in the offensive cyberoperations division of the US National Security Agency (NSA) see also B. Gellman, Dark Mirror, 2020, pp. 203–204.

75. Note that cybersecurity insurance is privately offered but, as with all insurance, subject to State regulation – an entry point for policy-making. Recent research indicates that, due to market dynamics, cybersecurity insurance is currently a weak form of non-State governance that fails to encourage minimum standards and regular auditing of cyber capabilities. Consultation with Daniel Woods, Security and Privacy Lab, University of Innsbruck; and D.W. Woods and T. Moore, "Does Insurance Have a Future in Governing Cybersecurity?", IEEE Security & Privacy, vol. 18, no. 1, 2019, pp. 21–27, https://doi.org/10.1109/MSEC.2019.2935702.

76. For an overview of attempts to mainstream gender into insurance, see K. Miles, M. Wiedmaier-Pfister and M.-C. Dankmeyer, Mainstreaming Gender and Targeting Women in Inclusive Insurance: Perspectives and Emerging Lessons, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), 2017, https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/gender+at+ifc/resources/women-in-inclusive-insurance. For an example of the complexity of insurance regulations and gender equality, see discussion of the EU Gender Directive on car insurance. P. Collinson, "How an EU Gender Equality Ruling Widened Inequality", The Guardian, 14 January 2017, https://www.theguardian.com/money/blog/2017/jan/14/eu-gender-ruling-car-insurance-inequality-worse; and European Commission, "EU Rules on Gender-Neutral Pricing in Insurance Industry Enter into Force", Press release, 20 December 2012, https://ec.europa.eu/commission/presscorner/detail/en/IP_12_1430.

77. J. Shires, "Enacting Expertise: Ritual and Risk in Cybersecurity", Politics and Governance, vol. 6, no. 2, 2018, pp. 31–40, http://doi.org/10.17645/pag.v6i2.1329.

78. See reports on the website of the Global Forum on Cyber Expertise (GFCE), https://thegfce.org/impact/. In the British context, as an example of recent research best practice in this area, see National Cyber Security Centre and KPMG, Decrypting Diversity: Diversity and Inclusion in Cyber Security, 2020, https://www.ncsc.gov.uk/report/diversity-and-inclusion-in-cyber-security-report.

79. S. Crislip, "Capturing Flags and Recruiting Future Cyber Soldiers", War on the Rocks, 28 August 2020, http://warontherocks.com/2020/08/capturing-flags-and-recruiting-future-cyber-soldiers/.

80. Professional cybersecurity roles vary greatly, ranging from technical design, hacking and coding positions via sales, marketing and human resources to diplomacy, regulation, law enforcement and advocacy. See Help Net Security, "Women are Increasingly Climbing the Cybersecurity Leadership Ladder", 3 April 2019, https://www.helpnetsecurity.com/2019/04/03/women-cybersecurity-workforce/; and S. Morgan, "Women Represent 20 Percent of The Global Cybersecurity Workforce in 2019", Cybercrime Magazine, 28 March 2019, https://cybersecurityventures.com/women-in-cybersecurity/.

81. Frost & Sullivan, 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, International Information System Security Certification Consortium, 2017, https://www.isc2.org/-/media/B7E003F79E1D4043A0E74A57D5B6F33E.ashx.

82. E. Dallaway, "Women in Cybersecurity: Proofpoint's Sherrod DeGrippo Answers Your Questions", Infosecurity Magazine, 15 July 2020, https://www.infosecurity-magazine.com/interviews/women-interview-sherrod-degrippo/.

83. See e.g. (with thanks to Beatrice Martini), Out in Science, Engineering, and Technology, https://ostem.org; Lesbians Who Tech, https://lesbianswhotech.org/debug2020/; Trans Tech, https://transtechsocial.org; Outreachy, https://outreachy.org; and Diana Initiative, https://dianainitiative.org.

84. E.g. Z. Homburger and L. Adamson, "CyCon 2018: From Cyber War to Toilet Lines", 11 June 2018, https://leidensecurityandglobalaffairs.nl/articles/cycon-2018-from-cyber-war-to-toilet-lines.

85. Importantly, however, such initiatives are often not intersectional. Despite the many women of colour from the Global South working in cybersecurity, such events frequently raise the visibility of predominantly White women from the Global North.

86. H. Metcalf, "Stuck in the Pipeline: A Critical Review of STEM Workforce Literature", InterActions: UCLA Journal of Education and Information Studies, vol. 6, no. 2, 2010, https://escholarship.org/uc/item/6zf09176. For a critique of the pipeline metaphor, see A. Vitores and A. Gil-Juárez, "The Trouble with 'Women in Computing': A Critical Examination of the Deployment of Research on the Gender Gap in Computer Science", Journal of Gender Studies, vol. 25, no. 6, 2015, http://doi.org/10.1080/09589236.2015.1087309.

87. D.T. Ireland et al., "(Un)Hidden Figures: A Synthesis of Research Examining the Intersectional Experiences of Black Women and Girls in STEM Education", Review of Research

in Education, vol. 42, no. 1, 2018, pp. 226–254; A. Sey and N. Hafkin (eds.), Taking Stock: Data and Evidence on Gender Digital Equality, United Nations University, March 2019, https://i.unu.edu/media/cs.unu.edu/attachment/4040/EQUALS-Research-Report-2019.pdf; UN News, "'The World Needs Science and Science Needs Women', UN Says on International Day", 11 February 2017, https://news.un.org/en/story/2017/02/551212-world-needs-science-and-science-needs-women-un-says-international-day; UNESCO Science Report, Towards 2030: Executive Summary, 2015, UNESCO, https://unesdoc.unesco.org/ark:/48223/pf0000235407; S. Cheryan et al., "Ambient Belonging: How Stereotypical Cues Impact Gender Participation in Computer Science", Journal of Personality and Social Psychology, vol. 97, no. 6, 2009, pp. 1045–1060, http://doi.org/10.1037/a0016239; and UNESCO Institute for Statistics (UIS), "Women in Science", Fact Sheet no. 55, June 2015, http://uis.unesco.org/sites/default/files/documents/fs55-women-in-science-2019-en.pdf.

88. S. Goy et al., "Swimming Against the Tide in STEM Education and Gender Equality: A Problem of Recruitment or Retention in Malaysia", Studies in Higher Education, vol. 43, no. 11, 2018, pp. 1793–1809, http://doi.org/10.1080/03075079.2016.1277383; and S.I. Islam, "Arab Women in Science, Technology, Engineering and Mathematics Fields: The Way Forward", World Journal of Education, vol. 7, no. 6, 2017, pp. 12–20, https://doi.org/10.5430/wje.v7n6p12.

89. S. Kahn and D. Ginther, Women and STEM, Working Paper no. w23525, National Bureau of Economic Research, June 2017, http://doi.org/10.3386/w23525. On cybersecurity specifically, see D. Peacock and A. Irons, "Gender Inequalities in Cybersecurity: Exploring the Gender Gap in Opportunities and Progression", International Journal of Gender, Science, and Technology, vol. 9, no. 1, 2017, http://genderandset.open.ac.uk/index.php/genderandset/article/download/449/824; and M. Carr and L. Tanczer, "UK Cybersecurity Industrial Policy: An Analysis of Drivers, Market Failures and Interventions", Journal of Cyber Policy, vol. 3, no. 3, 2018, pp. 430–444, https://doi.org/10.1080/23738871.2018.1550523; and A. Sey and N. Hafkin (eds.), Taking Stock: Data and Evidence on Gender Digital Equality, United Nations University, March 2019, https://i.unu.edu/media/cs.unu.edu/attachment/4040/EQUALS-Research-Report-2019.pdf.

90. F.J. García-Peñalvo, "Innovative Teaching Approaches to Attract, Engage, and Maintain Women in STEM: W-STEM Project", 2019, http://doi.org/10.5281/zenodo.3538939.

91. C. Glass and K.L. Minnotte, "Recruiting and Hiring Women in STEM Fields", Journal of Diversity in Higher Education, vol. 3, no. 4, 2010, pp. 218–229, https://doi.org/10.1037/a0020581.

92. E. Dallaway, Closing the Gender Gap in Cybersecurity, Crest, 2016, https://www.crest-approved.org/wp-content/uploads/CREST-Closing-the-Gender-Gap-in-Cyber-Security.pdf.

93. D. Bilimoria and L. Lord (eds.), Women in STEM Careers: International Perspectives on Increasing Workforce Participation, Advancement and Leadership, 2014.

94. S. Marlow and M. McAdam. "Analyzing the Influence of Gender upon High-Technology Venturing within the Context of Business Incubation", Entrepreneurship Theory and Practice, vol. 36, no. 4, July 2012, pp. 655–676, https://doi.org/10.1111/j.1540-6520.2010.00431.x.

95. J.L. Martínez-Cantos, "Digital Skills Gaps: A Pending Subject for Gender Digital Inclusion in the European Union", European Journal of Communication, vol. 32, no. 5, 2017, pp. 419–438, https://doi.org/10.1177/0267323117718464.

96. A. Sey and N. Hafkin (eds.), Taking Stock: Data and Evidence on Gender Digital Equality, United Nations University, March 2019, https://i.unu.edu/media/cs.unu.edu/attachment/4040/EQUALS-Research-Report-2019.pdf; and Organisation for Economic Co-operation and Development (OECD), Bridging the Digital Gender Divide: Include, Upskill, Innovate, 2018, http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf.

97. Ibid, p. 5.

98. S.B. Edwards and J.D. Duchess Harris, Hidden Human Computers: The Black Women of NASA, 2016; and C. Hooper, Manly States: Masculinities, International Relations, and Gender Politics, 2001; M. Hicks, Programmed Inequality: How Britain Discarded Women Technologists and Lost Its Edge in Computing, MIT Press, 2017; and J. Abbate, Recoding Gender: Women's Changing Participation in Computing, MIT Press, 2012.

99. M. Salter, "From Geek Masculinity to Gamergate: The Technological Rationality of Online Abuse", Crime, Media, Culture, vol. 14, no. 2, no. 247–264, https://doi.org/10.1177/1741659017690893; A. Adam, Gender, Ethics and Information Technology, 2005, https://doi.org/10.1057/9780230000520_7, pp. 128–146; and S. Brooke, "Breaking Gender Code: Hackathons, Gender, and the Social Dynamics of Competitive Creation", In Conference on Human Factors in Computing Systems, 2018, pp. 1–6.

100. T. Owen, W. Noble and F.C. Speed, "Virtual Violence: Cyberspace, Misogyny and Online Abuse", In New Perspectives on Cybercrime, 2017, pp. 141–158, https://doi.org/10.1007/978-3-319-53856-3_8; and A.A. Pescitelli, A. A., "MySpace or Yours? Homophobic and Transphobic Bullying in Cyberspace", Doctoral dissertation, Simon Fraser University, 2013, http://summit.sfu.ca/system/files/iritems1/13577/ETD7899_APescitelli.pdf.

101. C. Adams, "'They Go for Gender First' The Nature and Effect of Sexist Abuse of Female Technology Journalists", Journalism Practice, vol. 12, no. 7, 2018, pp. 850–869, https://doi.org/10.1080/17512786.2017.1350115.

102. A. Adam, Gender, Ethics and Information Technology, 2005, https://doi.org/10.1057/9780230000520.

103. Frost & Sullivan, 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, International Information System Security

Certification Consortium, 2017, https://www.isc2.org/-/media/Files/Research/ISC2-Women-in-Cybersecurity-2017.ashx.

104. L.M. Tanczer, "Breaking with the Code of the 'Male-Only' Stereotype in Hacktivsim", Fiber: Werkstoff Für Feminismus Und Popkultur, vol. 23, no. 2, 2013, pp. 14–15.

105. National Cyber Security Centre and KPMG, Decrypting Diversity: Diversity and Inclusion in Cyber Security, 2020, https://www.ncsc.gov.uk/report/diversity-and-inclusion-in-cyber-security-report.

106. E.g. W.R. Poster, "Cybersecurity Needs Women", Nature, 26 March 2018, https://www.nature.com/articles/d41586-018-03327-w. There is some evidence that this may be changing. P. Roberts, "Forget 'Brogrammers', Women Have the Edge in DEFCON Social Engineering Contest", Threat Post, 21 May 2012, https://threatpost.com/forget-brogrammers-women-have-edge-defcon-social-engineering-contest-052112/76587/.

107. A.P. Harris, "Race and Essentialism in Feminist Legal Theory", Stanford Law Review, vol. 42, no. 3, February 1990, pp. 581–616, https://doi.org/10.2307/1228886.

108. E. Dallaway, Closing the Gender Gap in Cybersecurity, Crest, 2016, https://www.crest-approved.org/wp-content/uploads/CREST-Closing-the-Gender-Gap-in-Cyber-Security.pdf; and Organisation for Economic Co-operation and Development (OECD), Bridging the Digital Gender Divide: Include, Upskill, Innovate, 2018, http://www.oecd.org/internet/bridging-the-digital-gender-divide.pdf, p. 15.

109. Fortinet, "Exploring the Benefits of Gender Diversity in Cybersecurity", 4 October 2019, https://www.fortinet.com/blog/business-and-technology/exploring-benefits-gender-diversity-cybersecurity.

110. See various networks of women in cybersecurity, including GFCE Gender Forum, Dutch Women in Cybersecurity (WiCS), Women in Cybersecurity (WiCyS), Women CyberSecurity Society, and Women Cyber Forum. See also National Cyber Security Centre and KPMG, Decrypting Diversity: Diversity and Inclusion in Cyber Security, 2020, https://www.ncsc.gov.uk/report/diversity-and-inclusion-in-cyber-security-report.

111. W.R. Poster, "Cybersecurity Needs Women", Nature, 26 March 2018, https://www.nature.com/articles/d41586-018-03327-w.

112. Consultation with Julia Slupska, University of Oxford.

113. W.R. Poster, "Cybersecurity Needs Women", Nature, 26 March 2018, https://www.nature.com/articles/d41586-018-03327-w.

114. For an illustration of the roles and skills associated with men and women in US cybersecurity, see C. Martinez, "Cybersecurity: Why You Should Care About the Skills and Gender Gap", Steppingblocks, https://blog.steppingblocks.com/cyber-security-gender-and-skills-gap.

115. Consultation with experts suggests that women in the Balkans and the former Soviet Union, for instance, may be better represented in State cyber positions than in the private sector. It would be useful to know if this is true (and if so, why), whether this translates into meaningful participation and whether it might offer useful lessons for other contexts.

116. L. Maschmeyer, R.J. Deibert and J. R. Lindsay, "A Tale of Two Cybers – How Threat Reporting by Cybersecurity Firms Systematically Underrepresents Threats to Civil Society", Journal of Information Technology & Politics, 2020; and I. Lopez-Neira et al., "'Internet of Things': How Abuse is Getting Smarter", Safe – The Domestic Abuse Quarterly, vol. 63, 2019, pp. 22–26, https://doi.org/10.2139/ssrn.3350615. For efforts to address this issue, see the Rapid Response Network, https://www.rarenet.org; and CiviCERT, https://www.civicert.org.

117. E.g. data for the USA: Statista, "Percentage of Employed Women in Computing-Related Occupations in the United States from 2000 to 2019", https://www.statista.com/statistics/311972/us-women-computer-workers/; and for the EU: Eurostat, "ICT Specialists in Employment", October 2019, https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_specialists_in_employment#ICT_specialists_by_sex.

118. L.M. Tanczer, I. Brass and M. Carr, "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy", Global Policy, vol. 9, no. S3, November 2018, pp. 60–66, https://doi.org/10.1111/1758-5899.12625. See especially remarks that CSIRTs further a "global expert culture and carry out important community building processes" (p. 62) and that they incorporate "delicate . . . cultural differences" (p. 63).

119. P. Hinojosa, K. Aiken and L.M. Hurel, "Putting the Technical Community Back into Cyber (Policy)", In E. Tikk and M. Kerttunen (eds.), Routledge Handbook of International Cybersecurity, 2020, pp. 326–340; and L.M. Tanczer, I. Brass and M. Carr, "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy", Global Policy, vol. 9, no. S3, November 2018, pp. 60–66, https://doi.org/10.1111/1758-5899.12625.

120. B.J. Strawser and D.J. Joy, "Cyber Security and User Responsibility: Surprising Normative Differences", Procedia Manufacturing, vol. 3, 2015, pp. 1101–1108, https://doi.org/10.1016/j.promfg.2015.07.183; K. Renaud et al., "Is the Responsibilization of the Cyber Security Risk Reasonable and Judicious?", Computers & Security, vol. 78, September 2018, pp. 198–211, https://doi.org/10.1016/j.cose.2018.06.006; and E.A. Jane, "Gendered Cyberhate, Victim-Blaming, and Why the Internet is More Like Driving a Car on a Road Than Being Naked in the Snow", In E. Martellozzo and E.A. Jane, Cybercrime and Its Victims, 2017, pp. 61–78.

121. D.W. Woods and T. Moore, "Does Insurance Have a Future in Governing Cybersecurity?", IEEE Security & Privacy, vol. 18, no. 1, 2019, pp. 21–27, https://doi.org/10.1109/MSEC.2019.2935702.

122. Consultation with Daniel Woods, Security and Privacy Lab, University of Innsbruck.

123. K. Miles, M. Wiedmaier-Pfister and M.-C. Dankmeyer, Mainstreaming Gender and Targeting Women in Inclusive Insurance: Perspectives and Emerging Lessons, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), 2017, https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/gender+at+ifc/resources/women-in-inclusive-insurance.

124. E.g. the European Union's Network and Information Security Directive requires its member States to have national cybersecurity capabilities related to preparedness, such as having a national CERT and performing cyber exercises.

125. Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, General Assembly, A/70/174, 22 July 2015, http://undocs.org/A/70/174, paragraph 17(e).

126. Ibid, paragraph 13(h).

127. Council on Foreign Relations, "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet", 13 January 2020, https://www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet.

128. This might be partially attributed to the lack of unified positions on how international law actually applies to cyberoperations. For the analysis of State's positions on the application of international law see R. Przemysław, Application of International Law to Cyber Operations: A Comparative Analysis of States' Views, The Hague Program for Cyber Norms, March 2020, https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views.

129. D. Broeders, E. De Busser and P. Pawlak, "Three Tales of Attribution in Cyberspace: Criminal Law, International Law and Policy Debates", The Hague Program for Cyber Norms, April 2020, https://www.thehaguecybernorms.nl/research-and-publication-posts/three-tales-of-attribution-in-cyberspace-criminal-law-international-law-and-policy-debates.

130. E.g. in 2020, Germany charged a Russian hacker, who is allegedly an employer of the Russian Main Intelligence Directorate (GRU) for a 2015 attack on the German Parliament. See C. Cimpanu, "German Authorities Charge Russian Hacker for 2015 Bundestag Hack", 5 May 2020, https://www.zdnet.com/article/german-authorities-charge-russian-hacker-for-2015-bundestag-hack/.

131. D. Shoker, "Making Gender Visible in Digital ICTs and International Security", Report submitted to Global Affairs Canada, 2019, https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf; and D. Brown and A. Pytlak, Why Gender Matters in International Cyber Security, Women's International League for Peace and Freedom (WILPF) and the Association for Progressive

Communications (APC), April 2020, https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf.

132. "Gender Equality and Cybercrime/Cyber Violence", https://rm.coe.int/gender-mainstreaming-toolkit-15-gender-equality-and-cybercrime-cybervi/168092e9b4; and L. Sharland and H. Smith, "Cyber, Technology and Gender: What Are We Missing?", The Strategist, 12 June 2019, https://www.aspistrategist.org.au/cyber-technology-and-gender-what-are-we-missing/.

133. A. Nagle, Kill All Normies: Online Culture Wars from 4chan and Tumblr to Trump and the Alt-right, 2017; J.T. Darden, Tackling Terrorists' Exploitation of Youth, American Enterprise Institute, May 2019, https://www.un.org/sexualviolenceinconflict/wp-content/uploads/2019/05/report/tackling-terrorists-exploitation-of-youth/Tackling-Terrorists-Exploitation-of-Youth.pdf; S. Walby et al., Study on the Gender Dimension of Trafficking in Human Beings: Executive Summary, European Commission, 2016, https://ec.europa.eu/anti-trafficking/sites/antitrafficking/files/study_on_the_gender_dimension_of_trafficking_in_human_beings._executive_summary.pdf; and C. Chen, N. Dell and F. Roesner, "Computer Security and Privacy in the Interactions Between Victim Service Providers and Human Trafficking Survivors", In 28th {USENIX} Security Symposium ({USENIX} Security 19), 2019, pp. 89–104, https://www.usenix.org/system/files/sec19-chen-christine.pdf.

134. United Nations Office on Drugs and Crime, "Gender-Based Discrimination and Women in Conflict with the Law", July 2019, https://www.unodc.org/e4j/en/crime-prevention-criminal-justice/module-9/key-issues/1--gender-based-discrimination-and-women-in-conflict-with-the-law.html.

135. M. Campbell, "Access to Justice: A Facet of Gender Equality", Oxford Human Rights Hub, 19 August 2015, https://ohrh.law.ox.ac.uk/access-to-justice-a-facet-of-gender-equality/.

136. P. Davies, "Women, victims and crime", In P. Davies, P. Francis and C. Greer (eds.), Victims, Crime and Society, 2007, pp. 165–201, http://doi.org/10.4135/9781446212202.n7.

137. S. Walklate, "Men, Victims and Crime", In Ibid, pp. 142–164, http://doi.org/10.4135/9781446212202.n6.

138. S.E. Ochs and K. Reed, "Victimizing Offenders and Criminalizing Victimhood: Narratives of Mass Incarceration in a 'Post-Racial' Era", Narrative and Conflict: Explorations in Theory and Practice, vol. 4, no. 1, 2016, pp. 1–42; and S. Cowan and R. Hewer, "Vulnerability, Victimhood and Sex Offences", In C. Ashford (ed.), Research Handbook on Gender, Sexuality and the Law, 2020.

139. B.K. Payne, "Defining Cybercrime", In T.J. Holt and A.M. Bossler (eds.), The Palgrave Handbook of International Cybercrime and Cyberdeviance, 2020, pp. 3–25, https://doi.org/10.1007/978-3-319-90307-1_1-1.

140. D.K. Citron, "Law's expressive value in combating cyber gender harassment", Michigan Law Review, vol. 108, no. 3, 2009, pp. 373–415, https://repository.law.umich.edu/mlr/vol108/iss3/3; and R.J. Dreke, L. Johnson and J. Landhuis, "Challenges with and Recommendations for Intimate Partner Stalking Policy and Practice: A Practitioner Perspective", Journal of Family Violence, vol. 35, no. 7, October 2020, https://doi.org/10.1007/s10896-020-00164-2.

141. R.J. Deibert and I. Poetranto, "Submission of the Citizen Lab (Munk School of Global Affairs, University of Toronto) to the United Nations Special Rapporteur on Violence Against Women, Its Causes and Consequences, Ms. Dubravka Šimonović", 2017, https://citizenlab.ca/wp-content/uploads/2017/11/Final-UNSRVAG-CitizenLab.pdf, p. 15.

142. "Gender Equality and Cybercrime/Cyber Violence", https://rm.coe.int/gender-mainstreaming-toolkit-15-gender-equality-and-cybercrime-cybervi/168092e9b4.

143. Consultation with SafetyNet Team at US National Network to End Domestic Violence.

144. BBC News, "Rape Victims Among Those to be Asked to Hand Phones to Police", 29 April 2019, https://www.bbc.com/news/uk-48086244.

145. S. Larsson, "The Socio-Legal Relevance of Artificial Intelligence", Droit et société, no. 103, 2019, pp. 573–593, https://doi.org/10.3917/drs1.103.0573.

146. J.O. Baker and A.L. Whitehead, "God's Penology: Belief in a Masculine God Predicts Support for Harsh Criminal Punishment and Militarism", Punishment & Society, vol. 22, no. 2, 2020, pp. 135–160, https://doi.org/10.1177/1462474519850570; and S. Tomsen, "Masculinities, Crime and Criminalisation", In T. Anthony and C. Cunneen (eds.), The Critical Criminology Companion, 2008, pp. 94–104.

147. E.g. the 2014 Apple iCloud hacking incident resulted in the non-consensual publication of celebrities' nude photographs. E. Grinberg and N. Chavez, "Connecticut Man Sentenced in Celebrity Photo Hacking Scandal", CNN, 30 August 2018, https://edition.cnn.com/2018/08/29/entertainment/celebrity-photo-hacking-sentence/index.html. On sextortion see B. Wittes et al., "Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault", Brooking Institution, 11 May 2016, https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/.

148. T.J. Kasperbauer, "Protecting Health Privacy Even When Privacy is Lost", Journal of Medical Ethics, vol. 46, no. 11, 2019, http://doi.org/10.1136/medethics-2019-105880.

149. Privacy International, "Why Does Reproductive Health Surveillance in India Need Our Urgent Attention?", 24 February 2020, https://privacyinternational.org/long-read/3368/why-does-reproductive-health-surveillance-india-need-our-urgent-attention; and J. Davis, "300,000 Records Breached in Ransomware Attack on Pennsylvania Health System", Healthcare IT News,

26 July 2017, https://www.healthcareitnews.com/news/300000-records-breached-ransomware-attack-pennsylvania-health-system.

150. BBC News, "Trans Charity Mermaids UK 'Deeply Sorry' for Data Breach", 16 June 2019, https://www.bbc.co.uk/news/uk-48652970; and C. Fox, "Gender Identity Clinic Leaks Patient Email Addresses", BBC News, 6 September 2019, https://www.bbc.co.uk/news/technology-49611948.

151. R. Saad, "Egypt's Draft Cybercrime Law Undermines Freedom of Expression", Atlantic Council, 24 April 2015, https://www.atlanticcouncil.org/blogs/menasource/egypt-s-draft-cybercrime-law-undermines-freedom-of-expression/; and F. Gerry and C. Moore, "A Slippery and Inconsistent Slope: How Cambodia's Draft Cybercrime Law Exposed the Dangerous Drift Away from International Human Rights Standards", Computer Law & Security Review, vol. 31, no. 5, October 2015, pp. 628–650, https://doi.org/10.1016/j.clsr.2015.05.008.

152. C.L. Mason and S. Magnet, "Surveillance Studies and Violence Against Women", Surveillance & Society, vol. 10, no. 2, 2012, pp. 105–118, https://doi.org/10.24908/ss.v10i2.4094.

153. E.g. initiatives of the Inter-Parliamentary Union, Gender-Sensitive Parliaments: Executive Summary, 2011, http://archive.ipu.org/pdf/publications/gsp11ex-e.pdf.

154. UN Women, "Gender Mainstreaming", https://www.unwomen.org/en/how-we-work/un-system-coordination/gender-mainstreaming.

155. European Institute for Gender Equality, "Gender Analysis", https://eige.europa.eu/gender-mainstreaming/methods-tools/gender-analysis. See also the GBA+ tool and training process developed by the Canadian Government, Status of Women Canada, "What is GBA+", 28 October 2020, https://cfc-swc.gc.ca/gba-acs/index-en.html.

156. E.g. L.M. Tanczer, "The Government Published Its Draft Domestic Abuse Bill, But Risks Ignoring the Growing Threat of Tech Abuse", 25 February 2019, Medium, https://medium.com/policy-postings/the-government-published-its-draft-domestic-abuse-bill-but-risks-ignoring-the-growing-threat-of-368a6fb70a14. To develop and revise legal responses to cybersecurity incidents, national legislative bodies can employ existing tools such as guidelines developed by the OSCE or the Inter-Parliamentary Union on gender-sensitive legislative processes. See OSCE Office for Democratic Institutions and Human Rights, Making Laws Work for Women and Men: A Practical Guide to Gender-Sensitive Legislation, 2017, https://www.legislationline.org/download/id/7545/file/Guidelines_Practical_guide_gender_sensitive_legislation_en.pdf.

157. This is particularly true for the young men (and a smaller number of young women) who enter into cybercrime, hacking and vandalism before adulthood. R. Marcinauskaitė, I. Pukanasytė and J. Šukytė, "Cyber Security Issues: Problematic Aspects of Hacking", Journal of Security and Sustainability Issues, vol. 8, no. 3, March 2019, https://repository.mruni.eu/handle/007/15752.

# Gender approaches to cybersecurity: design, defence and response

Designed by Jan Ondrasek

**Gender approaches to cybersecurity** explores how gender norms shape specific activities pertaining to cybersecurity design, defence and response. In each of these three pillars, the research identifies distinct dimensions of cyber-related activities that have gendered implications and, thus, need to be considered from a gender perspective.

The report proposes recommendations for the incorporation of gender considerations throughout international cybersecurity policy and practice, so as to ensure that cybersecurity improves the security of people of all gender identities and expressions, as well as international peace and security. The ultimate conclusion is that these two levels of security cannot be separated.