***THE DOSSIER***

# Women, Peace, and Cybersecurity

*By Diana Park and Kinsey Spears*

## Executive Summary

Since the Women, Peace, and Security (WPS) agenda entered the discussion among policymakers three decades ago, the security environment has been transformed, in part due to innovations in information and communications technology (ICT). As the cyber policy community grapples with the implications of cyberspace, a uniquely human-constructed domain of warfare, there is ample opportunity for WPS engagement in these issues. Discussions have yet to evolve and expand around gender and cyberspace operations.

The U.S. 2019 WPS Strategy does not recognize outright the importance of integrating the cyber and WPS agendas into one coherent effort. It does, however, lay out a framework to illustrate how these two policy communities can begin a dialogue around common objectives. This report addresses this incongruence using the objectives laid out in the 2019 WPS strategy.

### Key Takeaways

- Marginalized groups, particularly girls and women, have less access to technology than boys and men. The gender gap in the broader cyber workforce has further implications for how technology itself continues to perpetuate gender-based bias, including in artificial intelligence and machine learning.

Palestinian female students attend the Arduino Applications training at Spark for Innovation and Creativity in Gaza City on February 28, 2023. (Photo by Majdi Fathi/NurPhoto via Getty Images)

- Gender amplifies the human security implications of cyberspace, such as digital privacy, radicalization, harassment, gendered disinformation, or abuse that occur virtually, as well as physical violence that is directly impacted by policies and actions in cyberspace.

- There have been some calls for action from national and international actors on improving the integration of cybersecurity into the WPS agenda and vice versa. However, globally there is limited traction on incorporating cybersecurity and cyber threats into WPS National Action Plans or bringing WPS into relevant cybersecurity policies and initiatives.

## Policy Recommendations

**1.** The National Strategy for Women, Peace, and Security, which is currently being updated and revised, must include cyber considerations. Each implementing agency (the U.S. departments of State, Homeland Security, and Defense, as well as the U.S. Agency for International Development) should include actionable changes on WPS and cybersecurity in their agency-specific implementation plans.

**2.** The WPS and cybersecurity agenda must more robustly include cybersecurity, and the White House and the U.S. government's cybersecurity community need to be more active in incorporating WPS and gender analysis into their strategies.

**3.** Increase hiring for WPS and cybersecurity experts, including at the Office of the National Cyber Director and The Cybersecurity and Infrastructure Security Agency.

**4.** The U.S. needs to work with its allies and partners to incorporate WPS considerations into *all* cybersecurity measures at the United Nations.

**5.** The Biden administration needs to take an aggressive approach to tackling data privacy, especially given evolving threats to data and privacy protections on reproduction and sexual health information across the country.

**6.** The WPS community should play a leading role in investigating the overlap between gender and atrocity prevention in cyberspace. With a more robust understanding of the ways that gender-based harassment and threats play out online, the WPS agenda should engage more fully with its cyber policy counterparts to explore how technology can play a role in early warning and prevention.

JUNE 2023

THE DOSSIER

# Women, Peace, and Cybersecurity

*By Diana Park and Kinsey Spears*

NEW LINES
INSTITUTE
FOR STRATEGY AND POLICY

# Table of Contents

The views expressed in this article are those of the authors and not an official policy or position of the New Lines Institute.

COVER PHOTO: Women holding placards reading "Protect our freedom" demonstrate against controversial new surveillance laws in April 2015 in Paris. This was three months after Islamist attacks in Paris killed 17 people. The French government was debating new laws that allow the collection of data from suspected jihadists. The laws sparked a firestorm of protest from rights groups who say they infringe on individuals' privacy. (Eric Feferberg / AFP via Getty Images)

**The New Lines Institute for Strategy and Policy**

**Our mission** is to provoke principled and transformative leadership based on peace and security, global communities, character, stewardship, and development.

**Our purpose** is to shape U.S. foreign policy based on a deep understanding of regional geopolitics and the value systems of those regions.

## Introduction

As the Women, Peace, and Security (WPS) agenda matures into its third decade as a focus of policy implementation in countries around the world, the U.S. will mark the fifth anniversary of federal legislation that solidified WPS as a fixture in its national security considerations. The U.S. is also currently working to develop a new WPS national strategy set to be released in the fall of 2023. These temporal markers offer an opportunity to review the centrality of WPS within the backdrop of a rapidly transforming security environment, particularly in cyberspace.

The modernization of warfare in the past decades cannot be discussed without its key disruptive agent: innovations in information and communications technology (ICT). From the birth of a network that became the precursor to the Internet at the Advanced Research Projects Agency (later renamed Defense Advanced Research Projects Agency, or DARPA), to the deployment of artificial intelligence (AI) and machine learning into warzones, warfare has transformed, but has also been transformed by, the rapidly evolving ICT ecosystems driving today's society. Indeed, the battlefield itself has changed as a result. Whereas traditional domains of warfare had been limited to air, land, and sea, today's domains now include space and cyberspace.

Of these, cyberspace is unique because it is the only domain that cannot be neatly described in physical terms. The U.S. Department of Defense defines cyberspace as "a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the internet, telecommunications networks, computer systems, and embedded processors and controllers." Unlike the other domains, cyberspace cannot easily be isolated into neatly delimited militarized zones in which states challenge each other for dominance. The protocols that govern the way information is transmitted in cyberspace necessitate that preparations of the battlefield include civilian infrastructure, as well as a consideration of the social milieu that is manifest in cyberspace.

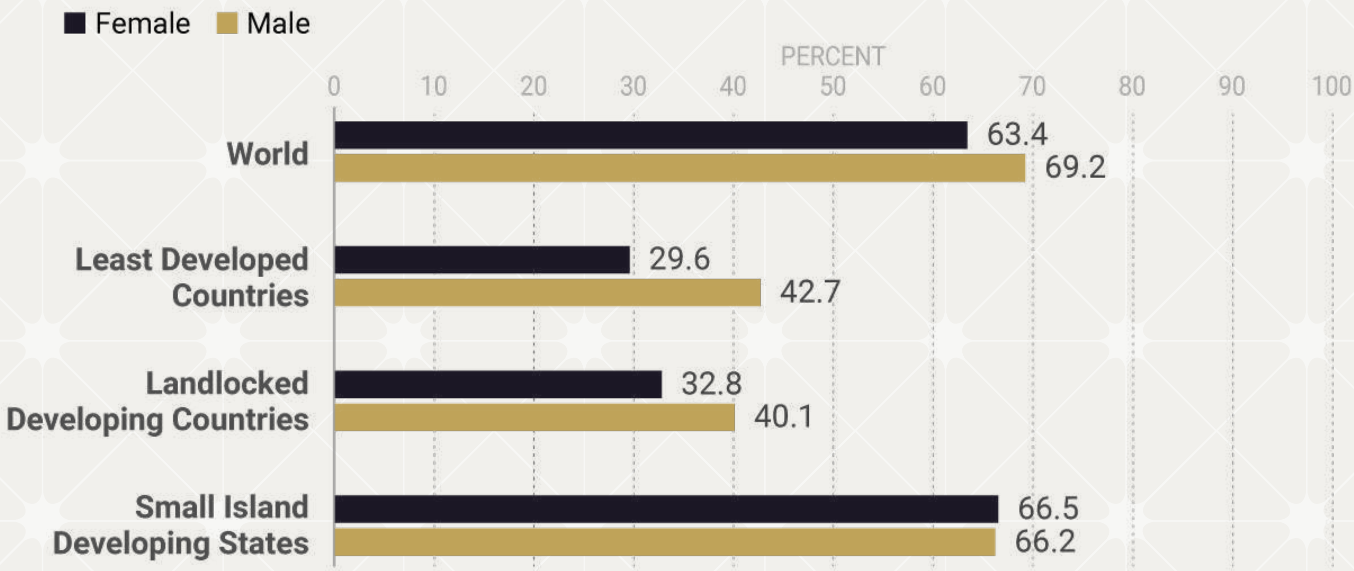
Lin Yi (second from left), head of the Chinese delegation for the 67th session of the Commission on the Status of Women, attends a China-EU side event on 'Fostering Women Entrepreneurship in Tech & Digital Sectors' at U.N. Headquarters on March 7, 2023 in New York City. (Liao Pan / China News Service / VCG via Getty Images)

Since the 2016 U.S. presidential election, more attention has been given to the implications of the cyberspace domain beyond just the technical applications and toward a more human-centered lens in its recognition of information operations as a critical military activity with cyber operations as one of its major components. In considering the role cyber capabilities can play in influencing the adversary's decision making through a full spectrum of information related activities, including psychological operations, the United States will still need to grapple with how information operations enabled through cyberspace might be executed, such as force structure and legal authorities. The increasing focus on a human-centered perspective on cyberspace in an industry otherwise dominated by technical analysis provides an opportunity for the WPS community to engage and expand on discussions around gender and cyberspace operations.

Because cyberspace is the only human-constructed war-fighting domain (its counterparts being land, air, sea, and space), there is significant room for the WPS community to explore in further depth the

## Female vs. Male Usage of the Internet Globally, 2022

The gender divide of internet use becomes more apparent in less-developed countries.



- **Least Developed Countries:** Afghanistan, Angola, Bangladesh, Benin, Bhutan, Burkina Faso, Burundi, Cambodia, Central African Republic, Chad, Comoros, Democratic Republic of the Congo, Djibouti, Eritrea, Ethiopia, Gambia, Guinea, Guinea-Bissau, Haiti, Kiribati, Lao People's Dem Republic, Lesotho, Liberia, Madagascar, Malawi, Mali, Mauritania, Mozambique, Myanmar, Nepal, Niger, Rwanda, Sao Tome and Principe, Senegal, Sierra Leone, Solomon Islands, Somalia, South Sudan, Sudan, Timor-Leste, Togo, Tuvalu, Uganda, United Republic of Tanzania, Yemen, Zambia.
- **Landlocked Developing Countries:** Afghanistan, Armenia, Azerbaijan, Bhutan, Botswana, Burkina Faso, Burundi, Central African Republic, Chad, Eswatini, Ethiopia, Kazakhstan, Kyrgyzstan, Lao People's Dem Republic, Lesotho, Malawi, Mali, Mongolia, Nepal, Niger, North Macedonia, Paraguay, Plurinational State of Bolivia, Republic of Moldova, Rwanda, South Sudan, Tajikistan, Turkmenistan, Uganda, Uzbekistan, Zambia, Zimbabwe
- **Small Island Developing States:** Small Island Developing States, Antigua and Barbuda, Bahamas, Barbados, Belize, Cabo Verde, Comoros, Cook Islands, Cuba, Dominica, Dominican Republic, Fiji, Grenada, Guinea-Bissau, Guyana, Haiti, Jamaica, Kiribati, Maldives, Marshall Islands, Micronesia (Federated States of), Mauritius, Nauru, Niue, Palau, Papua New Guinea, Samoa, São Tomé and Príncipe, Singapore, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, Seychelles, Solomon Islands, Suriname, Timor-Leste, Tonga, Trinidad and Tobago, Tuvalu, Vanuatu

**Note:** Some Landlocked Developing Countries and Small Island Developing States are listed as Least Developed Countries

Source: International Telecommunications Union, U.N.

© 2023, The New Lines Institute for Strategy and Policy

relationship between cyberspace and gender, with even greater implications for policies to be advanced both domestically and internationally. In turn, there is ample opportunity for cyber leadership in national security to recognize that advancing the national interest will gain greater success by working through and advancing WPS goals within its cyber strategy. Initiating a conversation between the WPS and cyber communities may recognize that they share a common vision of a cyberspace environment that is free and democratic. There is potential for both communities to work together toward advancing fundamental human rights for people of all genders while recognizing the significant progress to be made to create a more equitable existence for the most marginalized individuals in cyberspace.

A look at past Department of Defense and White House cyber strategies shows that there has been little, if any, discussion on how cybersecurity overlaps with the WPS agenda or a gender analysis.

### Cyber and the WPS Agenda

The WPS agenda in the United States has had different permutations, starting with the 2011 National Action Plan (NAP), to an updated NAP in 2016, the 2017 WPS legislation, and most recently the 2019 United States Strategy on Women, Peace, and Security. The 2011 NAP, the 2017 law, and the 2019 strategy make no mention of the internet, digital access, cyberspace, or cybersecurity. The 2016 NAP addresses some aspects of the cyber domain, such as the digital divide and the value of the internet for access to information. There is thus much work to be done on the inclusion of cyber discussions into WPS and vice versa.

While the 2019 WPS Strategy does not address outright the importance of cyber, WPS, and gender analysis, the strategy does lay out three objectives that apply to cyberspace and cybersecurity considerations.

These strategic objectives from the 2019 strategy aim to make demonstrable progress (defined below) by 2023:

> "Women are **more prepared and increasingly able** to participate in efforts that promote stable and lasting peace;
>
> Women and girls are **safer, better protected, and have equal access** to government and private assistance programs, including from the United States, international partners, and host nations; and
>
> United States and partner governments have **improved institutionalization and capacity** to ensure WPS efforts are sustainable and long-lasting."

These objectives highlight the importance of increasing women's access to and participation in securing peace and security; ensuring greater security and protection for women and girls; and formalizing WPS into greater permanence in government programs and policies.

Investments in STEM education for women and girls and greater recruitment of women into the tech and cybersecurity sector have already been on the forefront of the cyber workforce agenda. Greater scrutiny of cyberspace being used as a means of sexual abuse and harassment has opened a dialogue among cybersecurity experts about the gendered nature of online safety. These and other parallel efforts within the cyber community can aid in identifying additional common priorities between the two fields and contribute to additional areas where WPS can be further institutionalized into cyberspace considerations.

At present, the 2019 strategy is the guiding document for meaningful WPS integration across the U.S. government. However, as per the 2017 legislation, a new strategy is being developed across the interagency, leaving ample room to incorporate the cyber domain into WPS work. This is vital because the overarching cyber policies released by the current administration, most notably the recently released National Cyber Security Strategy, are woefully lacking in incorporating the WPS agenda. Using the 2019 strategy's objectives, the authors lay out a vision for how WPS can be integrated into cyber policies and vice versa.

## Objective 1: Increasing Women's Access to and Participation in Securing Peace and Security

One of the clearest examples of how gender has an impact on, and is impacted by, the digital space is in the digital divide. Marginalized groups, particularly girls and women, have less access to technology than boys and men. Globally, 69% of men use the internet compared to 63% of women, and those numbers are even more skewed in developing countries: In 32 low- and lower-income countries, the divide increases to an almost 52% differential in men's access to the internet compared to women. The reasons underpinning the digital divide are numerous, such as socio-cultural factors, inequitable literacy rates, affordability concerns, and geographic limitations.

This divide will continue to promulgate gender, racial, ethnic and class inequality globally; some reports say it has gotten worse in recent years particularly among rural households, in part due to COVID-19. Without equitable access, women and girls have fewer employment and educational opportunities, are less likely to be civically engaged, and have limited access to important health and safety information. The digital divide's impact on access to information for marginalized communities was laid bare during the pandemic, when safety and health information was primarily available online and employment opportunities became increasingly virtual.

The digital divide further perpetuates educational and career opportunities for women and girls in this sector. An International Information System Security Certification Consortium study surveying participants from North America, Africa, and the Asia-Pacific, found

WOMEN AND GIRLS FACE HARASSMENT AND ABUSE ONLINE!
BEWARE! ABUSE NOT TAKEN SERIOUSLY
CAUTION! WOMEN AND GIRLS AT RISK
DANGER!
RISK OF HARM!
DANGER!
SOCIAL MEDIA COMPANIES ARE NOT PROTECTING WOMEN AND GIRL
WARNING
WARNING! NO PROTECTION FOR WOMEN OR GIRLS
PUBLIC WARNING ISSUED BY REFUGE
WOMEN AND GIRLS ARE NOT SAFE ONLINE. THERE IS AN OPPORTUNITY TO CHANGE THIS. VIA THE ONLINE SAFETY BILL. BY ADDING IN A SPECIFIC VIOLENCE AGAINST WOMEN AND GIRLS (VAWG) CODE OF PRACTICE. THE GOVERNMENT COULD MAKE ONLINE SPACES SAFER FOR WOMEN AND GIRLS. MORE THAN 1 IN 3 WOMEN IN THE U.K. HAVE EXPERIENCED ONLINE ABUSE OR HARASSMENT ON SOCIAL MEDIA OR ANOTHER ONLINE PLATFORM.
IT'S TIME TO CHANGE THAT.
HELP ENSURE WOMEN AND GIRLS CAN STAY ONLINE SAFELY AND CONFIDENTLY.
Refuge

Reality television personalities Georgia Harrison (L) and Sharon Gaffka pose for photographs during an event calling for better online protections for women and girls. The Online Safety Bill was moving to the committee stage in the House of Lords on April 19, 2023 in London. Harrison's former partner Stephen Bear was sentenced to 21 months and placed on the sex offenders register in March, after he shared a sex video of the couple online without her consent. Sharon Gaffka was rendered unconscious and taken to a hospital after her drink was spiked at a restaurant in 2020. (Leon Neal / Getty Images)

that women make up only 24% of the cybersecurity workforce. At the Department of Homeland Security (DHS), Jen Easterly, the director of Cybersecurity and Information Security Agency (CISA), has been working to address this gender gap common in both the private and public sectors. Since her appointment, she has spearheaded numerous efforts to work within the federal government and with the private sector and civil society to increase access and opportunities for women in the field of cybersecurity. On March 8, CISA signed a Memorandum of Understanding (MoU) with Women in CyberSecurity, a nonprofit organization dedicated to women's representation and advancement in the field of cybersecurity. On March 13, CISA announced a similar partnership with the Girl Scouts of the United States of America to create greater access to cybersecurity and technological training for girls and young women.

Increasing women's recruitment and retention in the workforce may serve as a key solution as the field of cybersecurity continues to experience a severe shortage of professionals across all sectors, including at the Department of Defense (DoD). However, outside of CISA, there are seldom similar efforts replicated across the federal government. The DoD Cyber Workforce Strategy, signed Feb. 27 by Deputy Secretary of Defense Kathleen Hicks, while mentioning the importance of developing a diverse workforce, makes no explicit reference to a gender-based approach to addressing human capital shortfalls across its various functions, cyber information technology, cybersecurity, cyber intelligence, and cyber effects. The 2023 National Cyber Strategy takes a similar stance, making neither mention of the WPS agenda nor evidence of gender considerations part of the solution to fulfilling its strategic objectives. The word "women" appears once –and only in the context of addressing diversity in the workforce. More importantly, it fails to address the many factors that contribute to the systemic underrepresentation of women. For example, the findings and recommendations from the 2019 special report on women in STEM in the Federal Workforce by the U.S. Equal Employment Opportunity Commission provide evidence for a clear gender gap in the STEM workforce, particularly in technology, and lists the factors, such as harassment of women in this space, that have contributed to failed retention of women in the field.

The gender gap in the broader cyber workforce has implications for how technology itself continues to perpetuate gender-based bias. For example, bias in machine learning and AI are perpetuated throughout the industry. From the prevalence of female voice assistants like Alexa and Siri to hiring discrimination, there is a strong correlation between the gender gap in the workforce and gender-based bias in AI. AI generates patterns, predictions, and recommendations that are based largely on the humans that program them through machine learning. Human biases are inevitably coded into the technologies that we use today. Meanwhile, only 20% of technical jobs at major machine learning corporations are held by women and approximately 12% of AI researchers are women. Representational issues in the AI industry have been linked to harmful bias across all sectors in which algorithmic technologies have been implemented. For example, a drew attention to how the gender gap in the AI industry has led to most digital assistants and smart speakers being set to default female voices, reinforcing gender based biases around servility and femininity, while also programmed to respond flirtatiously back to sexually explicit prompts by the user. The issues around bias span across the sectors in which AI is employed, including facial recognition software, which is deployed across society, from personal digital devices to law enforcement. The Gender Shades project, led by Joy Buolamwini, found that facial recognition algorithms performed the worst on women with darker skin tones and pointed the wider psychosocial, physical, economical, and other real harms that AI posed on both individual and society. The underrepresentation of women across the cyber workforce will continue to impact everyday lives and, with emerging military applications of AI, will have lasting effects in the future of peace and security.

## Objective 2: Ensuring Greater Security and Protection for Women and Girls

Implications for WPS considerations in cyber expand beyond gaps in the workforce and biases in technology. On examining the human security implications of cyberspace, gender amplifies issues that impact individuals, such as digital privacy, radicalization, harassment, gendered disinformation, or abuse that occur virtually, as well as physical violence that is directly impacted by policies and actions in cyberspace. For the WPS community, to achieve this second objective would also entail a more concerted effort to engage with the cyber community on policy considerations on issues such as privacy, cybersecurity, and cyber violence against women and girls.

Misogyny and gendered violence in cyberspace have been directly linked to numerous instances of mass violence against women around the world. Facebook in particular has been used as a tool in multiple crises targeting women. In Myanmar, for example, the internet and social media were flooded with disinformation and propaganda, fueling extremist discourse and an increase in sexual and gender-based violence against women and girls during the recent military coup. Social media accounts were posting girls' photos without their consent, there was considerable slut-shaming and name calling towards young girls, and girls from ethnic and religious minority groups faced hate speech at alarmingly high rates. Cyberspace, particularly social media platforms, can serve as the primary domain in which information can be weaponized with implications for the physical domains – such as the case of Myanmar, inciting violence to the point of genocide – an inherently gendered crime. The WPS community, therefore, can play a larger role in advocating for the human security implications of cyber enabled information operations, particularly when executed by regimes that seek to contravene international norms on genocide and gender-based violence.

Policies around cyber governance, and in government approaches to ICT infrastructure regulation (or control, in the case of many authoritarian environments), also have a gendered dimension that is often overlooked in the debates and considerations that occur in the cyber community. China and Russia advocate for "cyber sovereignty" as a competing norm for Internet governance that normalizes censorship, information control, and repression in cyberspace under the auspices of non-interference. This is open defiance of the existing norms around a free and open internet. China in particular has demonstrated its ability to execute such a model through state-owned internet service providers, enforcing censorship tools and deploying surveillance tools against targeted populations. This enables the government to maximize its capabilities in cyberspace to suppress human rights. In the case of the Uyghurs, the specific targeting of women, as part of a systemic genocidal campaign against the ethnic and religious minority, is of particular concern when considering authoritarian control of the cyber domain.

While countries also continue to grapple with the proliferation of a range of cybercrimes, cyber violence against women and girls is occurring at alarming rates. By 15 years old, one in 10 women have already experienced a form of cyber violence.

Violence occurring in cyberspace facilitates and exacerbates crimes that are committed in the physical domain, in the form of sexual abuse, physical violence, or economic harm. For example, the Internet of Things, such as "smart" home technologies, wearable tech, and home assistants, have become avenues for technology-facilitated abuse wherein technology is used to stalk, harass, abuse, and control individuals. Technologies such as the Apple AirTag, smart tablets, and/or fitness trackers such as FitBits have all been used to stalk, harass, and commit intimate partner violence against women.

As countries continue to improve regulations around privacy and cybersecurity, these efforts will have additional implications for the security of women and

## Definitions of Gender-Based Cyber Crimes

Definitions are from the European Institute for Gender Equality publication: Gender-based violence, Combating Cyber Violence against Women and Girls.

| | |
|---|---|
| **Cyber stalking** | Cyber stalking is perpetrated by electronic or digital means. It is methodical, persistent and involves repeated incidents. It is perpetrated by the same person and undermines the victim's sense of safety. Cyber stalking includes offensive or threatening emails, text messages or instant messages; offensive comments posted on the internet; and intimate photos or videos shared on the internet or by mobile phone. |
| **Cyber harassment and cyber bullying** | Persistent harassment is aimed at a specific person, and is designed to cause severe emotional distress and often a fear of physical harm.<br>The focus of cyber bullying is almost exclusively children, adolescents, and young adults. It is characterized by legal and emotional vulnerability. |
| **Online gender based hate speech** | Hate speech is conduct publicly inciting violence or hatred against a group or a member of a group defined by race, color, religion, descent, or national or ethnic origin. Although online hate speech may not be different from similar expressions found offline, its challenges include regulation of its permanence, itinerancy, anonymity, and jurisdiction. |
| **Non-consensual intimate image abuse** | This form of abuse concerns publicly disseminating sexually explicit content without consent, especially by social networks. Most victims are women. It is often committed by a victim's former partner by posting on social media or adult content website. Permission to share these private images or videos was never granted. The motive may include revenge or other malicious intent. |

Note: There are of course other more specific versions of gender-specific harms that fall under the purview of cyber violence (doxxing, swatting, trolling, body shaming) but EIGE specifies that they fall under one of the above umbrella terms.

Source: European Institute for Gender Equality
https://eige.europa.eu/publications/combating-cyber-violence-against-women-and-girls

© 2023, The New Lines Institute for Strategy and Policy

girls in cyberspace. Advanced economies, following the European Union's adoption of the General Data Protection Regulation, the most comprehensive regulation to date for data privacy, have adopted similar approaches. However, the debate persists in the United States whether privacy regulation should remain sector-specific or all-encompassing, at the state or federal level. The lack of a comprehensive approach in the United States has grave implications for the safety and security of women. For example, after the 2022 Supreme Court ruling overturning Roe v. Wade, data stored on the cloud in period tracking applications can be subpoenaed to prosecute those violating anti-abortion laws in certain states. Data privacy across all platforms is critical; for example, Facebook gave private user data about an abortion to Nebraska police, which was then used to bring up criminal charges against two women.

There is ample opportunity for the WPS community to engage on the many underlying cyber policy issues that can have an impact on ensuring a free and open cyberspace environment for all, where women and girls can maneuver and engage without risk of violence. Increased multisectoral and international cooperation is necessary to combat the range of crimes, both enabled through cyberspace or crimes confined to the virtual domain, that often target women and girls. Recognizing the disproportionate harms that women, girls, people of color, and individuals with diverse SOGIESC (sexual orientation, gender identity or expression, and sexual characteristics) experience in cyberspace, the Biden administration established the White House Task Force to Address Online Harassment and Abuse. This task force aims to provide federal coordination, leadership, and resources toward preventing and addressing gender-based violence facilitated through cyberspace. WPS engagement on initiatives such as the State Department's Global Partnership for Action on Gender-Based Online Harassment and Abuse can draw on decades of experience in evidence-based programming and international engagement on complex, multi-sectoral issues affecting women and girls.

Gamergate, a harassment campaign led by men against women that lasted from 2014 to 2015, was a loosely organized and targeted campaign against feminists in gaming culture. It served as a watershed moment in the larger rise of the alt-right movement online. Although the campaign was originally rooted in hate speech toward women and was tenuously connected to video games, it was a jumping off point for much of the current online radicalization of young men, which played a role in the election of President Donald Trump in 2016. Gamergate continues to have an outsized impact on the radicalization of young men online and should have served as a wakeup call for those working on cybersecurity to the very real in-person capacity for violence from online forums. In particular, the doxing of women who subsequently had to leave their homes, cyberstalking, and revenge porn all had very real world consequences. Gamergate served as a launchpad for many of the online activities that led to the surge in the alt-right movement after 2016. A thorough gender analysis of this event could have served as a warning sign for how much gamergate serves as a political playbook for radicalization and online to offline organizing tactics.

In the United States, cyberspace has allowed alt-right movements to mobilize much quicker and easier than they have been able to in the past. Using apps like Parler, Signal, Gab, and Telegram, people affiliated with far-right organizations like The Three Percenters, Proud Boys, The Oath Keepers, and other openly avowed Nazis and white supremacists were able to plan and coordinate the storming of the U.S. Capitol on Jan. 6, 2021, that led to five deaths. The far-right demographic of America has become increasingly insular, receiving its news from networks like One American News Network and Newsmax, both of which spread lies that the 2021 presidential election was stolen. Gender identity and ideology is connected to violent extremism and terrorism; misogyny and hostility toward women are common elements in domestic terrorism cases in the U.S. The most significant terrorism threat to the U.S. is not foreign nationals, but homegrown white supremacists and other far-right extremists whose ideologies are based on racial and gender discrimination.

The WPS agenda must take cyber threats seriously, in both the everyday impact on women and girls and in its most extreme manifestations abetting atrocity crimes like genocide and crimes against humanity. According to the 1948 Genocide Convention, State signatories

Spanish astronaut Sara Garcia (left) of the European Space Agency, and Spain's Minister of Science and Innovation Diana Morant speak during at the 'Day of Women and Girls in Science: awakening STEM vocations' conference in Madrid, Spain. The Ministry of Science and Innovation celebrated the International Day of Women and Girls in Science on Feb. 11. (Eduardo Parra / Europa Press via Getty Images)

must respond to genocide, or the risk of genocide, at the very moment they became aware of the crime (or reasonably should have been aware). While the Internet makes it much easier to incite genocide and inflame existing inter-group tensions, it can also be utilized as a means of preventing these very crimes through tools designed for prevention and education.

## Objective 3: Formalizing WPS into Greater Permanence in Government Programs

There have been some calls for action from national and international actors on improving the integration of cybersecurity into the WPS agenda and vice versa. These calls have gained momentum recently both domestically and internationally. However, globally there is limited traction on incorporating cybersecurity and cyber threats into WPS National Action Plans or bringing WPS into relevant cybersecurity policies and initiatives. Only three National Action Plans mention cyber threats as a component of WPS work: Ireland, Namibia, and most recently the United Kingdom. In the U.N.'s 2021 Secretary-General report on WPS, there was an acknowledgement that to ensure gender equitable access maintaining security in both physical and digital spaces is necessary.maintaining In this report, there were also a few discussions on how the pandemic exacerbated gendered inequities in access on online platforms because during lockdown so many activities and employment opportunities were moved online. There are discussions happening at the global level on merging WPS and cybersecurity, but it is time to enshrine it in laws, resolutions, and plans. However, this is not a big enough step.

The links between WPS, gender, and cybersecurity go far beyond just sexual and gender-based violence (SGBV), and not enough additional U.S. government cybersecurity initiatives take gender into consideration. In 2021, President Joe Biden issued an Executive Order on Improving the Nation's Cybersecurity, which does not address gender-specific issues or how the WPS initiative can be a functional tool in such efforts. Additionally, the WPS National Strategy and the implementation plans for all four agencies (USAID and the U.S. departments of Defense, Homeland Security, and State) tasked with carrying out the agenda have no cybersecurity integration. While CYBERCOM has hired their first WPS adviser, a laudable first step, WPS and gender continue to be missing in the Command Vision

> “ By doxing NATO staff of all genders, but particularly women, Russia is potentially unleashing a wave of harassment that might affect their lives for years, just as women involved in Gamergate continue to be targeted years after the incident. ”

for U.S. Cyber Command and the 2018 Cyberspace Strategy Symposium Proceedings, both of which are the primary guiding documents available on the CYBERCOM website. While it is valuable to have cyber security as a component of the 2023 National Strategy on Gender Equity and Equality, it should not remain siloed away from broader cyber strategic planning, communication, and execution. It is time to bring more overlap between these fields and communities.

## WPS and Offensive Cyber Operations

While the Strategic Objectives from the 2019 National Strategy allow for clear guideposts on where to include cybersecurity and WPS analysis, additional considerations should be incorporated into both WPS and cyber strategies. Of particular concern is addressing gendered implications of offensive cyber operations by states or proxies in conflict. In the ongoing war in Ukraine, there is mounting evidence of actors targeting civilian infrastructure. A Ukrainian-aligned volunteer “army” operating in Ukraine, which calls itself the IT Army of Ukraine, recently targeted Chestny ZNAK, a digital tracking and authentication system for products made in Russia, including food and pharmaceutical products. Meanwhile, Russia has consistently attempted, though unsuccessfully due to Ukrainian cyber defenses, to target civilian infrastructure such as power grids and ICT equipment. Russian cyberattacks have also targeted NATO infrastructure, which included data exfiltration and subsequent doxing of NATO staff, releasing their email addresses to the public. All three of these types of attacks have serious gendered impacts.

The NATO doxing of staff puts women who are NATO staff members at heightened risk of cyber harassment, stalking, and abuse. By doxing NATO staff of all genders, but particularly women, Russia is potentially unleashing a wave of harassment that might affect their lives for years, just as women involved in Gamergate continue to be targeted years after the incident.

As in other components of security and conflict, there is room for rigorous gender analysis when discussing the offensive cyber operations’ targeting of civilian critical infrastructure that might affect power grids, telecommunications systems, and secure supply chains of food and medicine. In times of conflict and crisis, it is women who are most affected by decreasing access to consistent food. By Ukraine targeting Chestny ZNAK, the main food distribution mechanism in Russia, women are most vulnerable to food insecurity and hunger. The targeting of power grids also has lasting effects on marginalized individuals. People experiencing disabilities might be more reliant on a safe and consistent power grid, and it is typically women in a society who do the majority of caregiving for people experiencing disabilities. These snippets laying out the connection between marginalized groups and cyberattacks showcase just a few of the many reasons why targeting of civilian infrastructure in cyberspace should be of critical importance for the future of cybersecurity policies in the U.S.

## Recommendations

**1.** The National Strategy for Women, Peace, and Security is being updated and revised per the 2017 legislation. The previous Strategy did not include the internet or any discussion about cyberspace at all. The updated strategy, set to come out sometime in the fall of 2023, must engage cyber policy in a meaningful way. The importance of cybersecurity on WPS, and vice versa, is far-reaching. The overlap between the WPS agenda and the U.S.'s cyber policy goals are mutually reinforcing, particularly in the face of democratic backsliding, increased risks of SGBV online, and data breaches, each of which have specific gendered risks. Furthermore, each implementing agency should include actionable changes on WPS and cybersecurity in their agency-specific implementation plans.

**2.** The WPS agenda needs to more robustly include cybersecurity into its strategies and plans, and the White House and the U.S. government's cyber policy community need to be more active in incorporating WPS and gender analysis into their strategies. It is not enough for cyber to be addressed in the WPS strategies, as this only reinforces the siloing of the specific gendered harms of weak cybersecurity. While the most recent National Cybersecurity Strategy does address some vital aspects of a free and fair internet that would reinforce the goals of the WPS agenda, it needs to be more explicit in its discussion about women in STEM, cyber-based SGBV threats, and how the gendered dynamics of alt-right subgroups play out online leading to in-person national security threats.

**3.** Increase hiring for more WPS and cybersecurity experts. CYBERCOM hired its first WPS expert in 2022 and has held its first Gender Focal Point. These are critical steps to improving the government's knowledge and capacity on how WPS and cybersecurity are theoretically and operationally intertwined. Increased hiring at CYBERCOM is useful, but there also needs to be an increase in WPS-specific knowledge and skills in the Office of the National Cyber Director and The Cybersecurity and Infrastructure Security Agency.

**4.** In March 2023, the United Nations hosted its annual Committee on the Status of Women, CSW67, which focused on Innovation and Technological Change and Education in the Digital Age. This increased focus is timely because, as a United Nations Institute for Disarmament Research report noted in 2021, "none of the WPS resolutions contain references to 'cyber,' 'online,' 'technology,' 'digital' or 'internet,' nor to cyberspace or cybersecurity."

There have been other avenues that have addressed the importance of bringing a WPS focus into cyber, such as the Women, Peace and Cybersecurity: Promoting Women's Peace and Security in the Digital World a program being implemented by U.N. Women. However, like the siloing happening in the U.S. government, the overlap of cyber and WPS cannot be exclusively the purview of U.N. Women. The recent Open-Ended Working Group on ICTs needs to adequately address the WPS agenda in its report back to the General Assembly in 2025. The July 20 progress report from the chair of the working group does an adequate job of indicating both the involvement of women in the decision-making process and including gender perspectives in its discussions. However, the 2022 Annual Progress Report does not include any mention of WPS or gender.

The U.S. needs to work with its allies and partners to incorporate WPS into *all* cyber policy initiatives at the United Nations. None of the statements made by the U.S. vis-a-vis the OpenEnded Working Group address the lack of consideration for WPS and gender matters in the ongoing work. The U.S. needs to consistently put pressure on the U.N. to include WPS across all cybersecurity matters, particularly given the current climate in the Security Council and how unlikely a robust UNSCR on cyber and WPS would be.

**5.** The Biden administration needs to aggressively tackle data privacy given the almost daily changes in abortion restrictions across the country. People who get pregnant, and thus need medical abortion care, are at particular risk of DDOS attacks and other pernicious data breaches or even the outright sale of personal health data. The Biden administration needs to take aggressive legal measures to protect individuals' health data from data brokers who sell health and location information and install specific data and privacy protections on reproductive and sexual health information.

**6.** With a more robust understanding of the ways that gender-based harassment and threats play out online, the U.S. can better understand how to anticipate, respond to, or prevent atrocities. Social media, specifically targeting of women, has played a critical role in radicalization, extremism, and in-person violence. Despite this growing body of knowledge, the strategies most able to bridge the divide between WPS, cybersecurity, and atrocities are missing this analysis. The 2020 United States Strategy to Prevent Conflict and Promote Stability, the subsequent 2022 Prologue to the United States Strategy to Prevent Conflict and Promote Stability, and the 2022 United States Strategy to Anticipate, Prevent, and Respond to Atrocities all come up short in addressing the overlap between gender, cyber, and atrocity prevention. The WPS agenda could play a role in early warning and atrocity prevention and response, especially in the digital age where we can see warning signs and risk factors clearly playing out in front of our eyes in cyberspace.

**7.** A sustained commitment from the Gender Policy Council on the importance of Women, Peace, and Security as a component of cyber policies across the Biden administration is more critical now than ever leading into the 2024 U.S. presidential election.

For example, it is in the national interest to invest in greater attention to gender as a focus and a solution to the systemic shortages in the cybersecurity workforce. The security and resilience of the nation's critical infrastructure, which includes the defense industrial base, the communication sector, and the election infrastructure subsector, depends on the strength of the nation's cybersecurity posture. Without incorporating a gender lens into domestic and international cyber policymaking processes, this administration will fall woefully short on both its commitment to gender equality and cybersecurity.

**Diana Park** is a doctoral student of international relations at the Fletcher School. With a research focus at the intersection of international security studies and cybersecurity, her dissertation examines the impact of cyberspace on nonviolent civil resistance in authoritarian environments.

She brings extensive intelligence and foreign policy experience to her discipline, joining the Fletcher School after a career at the U.S. State Department, Treasury Department, and Office of the Secretary of Defense for Policy. She is also a veteran of the U.S. military with more than a decade of service in the Navy Information Warfare Community.

Diana earned a Master of Public Policy from the Harvard Kennedy School, graduated with a Master of Arts in Cybersecurity Technology from the University of Maryland, and completed a Bachelor of Science in Foreign Service from Georgetown University. She is a Tillman scholar with the Pat Tillman Foundation and has received a research fellowship on nonviolent resistance in cyberspace with the International Center on Nonviolent Conflict.

**Kinsey Spears** is a doctoral candidate at the Fletcher School of Law and Diplomacy at Tufts University, where her work focuses on gender and security studies. Spears is also a researcher for the Feinstein International Center; a Teaching Fellow at Tufts; and a Research Fellow at the World Peace Foundation. She has worked as a Director of Scheduling in the U.S. Senate. She tweets at @Kinspears.

## Contact

For media inquiries, email media@newlinesinstitute.org

To submit a piece to the New Lines Institute,
email submissions@newlinesinstitute.org

For other inquiries, send an email to info@newlinesinstitute.org

1776 Massachusetts Ave N.W. Suite 120
Washington, D.C. 20036

(202) 800-7302

## Connect With Us

@newlinesinst

@New Lines Institute for Strategy and Policy

Subscribe

Sign up

NEW LINES INSTITUTE
FOR STRATEGY AND POLICY