Women and Cybersecurity

Alana LOMÓNACO BUSTO and Patricia PRANDINI
Master in International Relationships and Negotiations (FLACSO-UDESA) Master in Cybersecurity (UBA)

Introduction

The protection of information and resources used for its management, is an issue that requires attention and concern for individuals as well as all types of organizations. The accelerated growth of threats, linked to both technical progress and the emergence of new opportunities, constitutes an imperative call to action at all levels, in order to seriously seek solutions that will mitigate the consequent risks.

Particularly during 2020, the harmful effects of covid-19 were reflected equally in both the physical environment and cyberspace. In effect, the impact of the materialization of threats such as ransomware, grooming and phishing, has increased during the pandemic. This was mainly due to the restriction of movement of people, both in the work and social environment, and the urgency with which the resulting problems had to be resolved.

In the context of the accelerated digitization brought by the pandemic, the centrality of cybersecurity for individuals, organizations and states is becoming increasingly evident. However, perhaps due to its novel nature and its constant evolution, there is still no international consensus regarding its conceptualization and the dimension of its scope.

ISO/IEC 27032:2012[1], the international organization for standardization (ISO) provides guidelines to improve the state of cybersecurity. It defines cybersecurity as the preservation in cyberspace of three properties of information: confidentiality, integrity and availability. In a side note, it extends this scope to authenticity, primary responsibility ("accountability"), non-repudiation and the reliability of information. We could say, using simple language, that cybersecurity deals with the protection of information in any format and medium, and with the defense of the rights of people and organizations in virtual environments, characterized by high connectivity between devices and entities.

As well as ambiguity surrounding the definition of cybersecurity, there is also no clarity regarding its scope. While part of the bibliography mostly concerns preventive aspects related to the resilience of technological systems and infrastructures, other authors assign it a more comprehensive dimension which includes the prosecution of cybercrime, the scope of the police and judicial forces, and cyber defense as a field of action of the Armed Forces.

The truth is that this discipline requires a multifaceted approach that covers not only technological aspects, but also legal, cultural and educational aspects among others.

At the organizational level, the centrality of cybersecurity for the business becomes more and more important every day and is strongly linked to the governance of information and processes. Carrying out cybersecurity functions also requires multiple skills and competencies and the requirement to constantly keep up to date on a diversity of topics and situations.

[1] ISO/IEC 27032:2012 *"Information technologies – Security techniques – Guidelines for Cybersecurity"*

The role of women in cybersecurity

Whether due to structural or historical inequalities, women are strongly underrepresented in this field equally in both the debates and the decision-making processes related to cybersecurity and cyber defense in the international arena.

As stated in the study "Why Gender Matters in international Cybersecurity" carried out by "Women's International League for Peace and Freedom" and "Association for Progressive Communications": "Gender matters in international cybersecurity. It shapes and influences online behavior; determines access and power; and is a factor of vulnerability. Much of what is known about gender and cybernetics comes from gender studies related to online violence and gender inequality in the ICT sector. Less is known about how malicious international cyber operations between states affect people differently based on gender or other characteristics that may put them in positions of vulnerability."

A 2017 report[2] by PWC (a UK consulting firm), based on interviews with 2,000 outstanding British students, indicated that only 3% of the participants stated that their first choice was a professional career in the area of 'STEM'. 78% could not name a relevant female figure to work in this field of action, while only 5% of management positions in the sector were held by women at that time.

In the field of information and communication technologies, most global studies place women at participation levels of between 15 and 20%, in all related professions.

In the field of cybersecurity specifically, according to figures from the International Information Systems Security Certification Consortium[3],(ISC)2, that are based on a study carried out in 2019, women who work in cybersecurity represent only 24% of the total workforce globally. In 2017, this proportion amounted to 11%. Although, it should be noted that the 13 percentage disparity was due to a difference in the methodology used in the survey which had broadened the range of disciplines and incorporated (in addition to computer science) others such as law, communication, education and organizational management.

Finally, an American academic study[4] concerning the low participation of women in cybersecurity in the USA found that stereotypes and biases negatively influence women who work in this profession; it also identified that early exposure to cybersecurity is key when it comes to generating interest in women and finally the study confirmed that men occupy most of the key positions that influence the entry of professionals to workplaces in this field.

International Perspective

Since 1998, under the topic "Advancement of Information and Communication Technologies (ICT) in the context of international security", the United Nations have handled issues that concern cybersecurity, the application of international law in cyberspace, cyber defense, norms, rules and principles that should guide the responsible behavior of States in cyberspace, the protection of critical infrastructures and others. The main objective is to prevent conflicts or threats that, through the use of cyberspace as a means or objective, could put international peace and security at risk.

According to the study "Gender in Cyber Diplomacy" carried out by the United Nations Institute for Disarmament Research (UNIDIR), across the 6 Groups of Government Experts on the advancement of

[2] PwC. (2017). *"Time to close the gender gap"*. Available at: https://www.pwc.co.uk/who-we-are/women-in-technology/time-to-close-the-gender-gap.html

[3] (ISC)2. (2018). *"Women in cybersecurity"*. Available at: https://www.isc2.org/-/media/ISC2/Research/ISC2-Women-in-Cybersecurity-Report.ashx

[4] Sturhonda, J. (2019). *"The underrepresentation of females in the united states cybersecurity workforce: a multiple-case study"*. Available at: https://search.proquest.com/openview/524ae453b5af718568bcf782065a4817/1?pq-origsite=gscholar&cbl=18750&diss=y

ICT in the context of international security (GGE) that have been convened in the last 15 years, women have only represented an average of 20.2% of the participants. Only 10% of women were in the 1st GEG and this amount increased to 20% in the 5th GEG. This figure has only been surpassed in the 6th GEG -being close to 40% - in line with the commitment expressed by the UN Secretary General to achieve gender parity "in all the panels, boards and groups of experts established under its auspices in the field of disarmament" as contained in Action 37 of its 2018 Agenda for Disarmament[5].

At the 1st session of the United Nations Open Ended Working Group (OEWG) on the advancement of ICT in the context of international security in September 2019, 32% were women and 68% were men and only 24% of the delegations were headed by women. At the 2nd session of the OEWG in February 2020, the proportion was 39% women and 61% men, and 119 statements (out of a total of 280) were delivered by women.

Conclusion

It is necessary to recognize that technology reflects the values and biases of those who develop it. Consequently, failing to reverse trends that show a gender bias inevitably carries the risk of further consolidating, and even amplifying, the stereotypes and inequalities that exist today.

On the other hand, gender diversity is a means of increasing the plurality of perspectives. Various studies have shown that decision-making bodies diverse in composition are more effective in terms of risk assessment and problem solving because they perform more careful information processing. In the field of international peace and security, UN WOMEN has highlighted that the significant participation of women in the negotiation tables allows organizations to reach more lasting and sustainable agreements.

Women face different threats in the context of cybersecurity and can therefore contribute their visions and priorities to the discussions. In this context, it is necessary to understand the causes and consequences of gender gaps in the field of cybersecurity, both at a technical and decision-making level, as well as in international and regional cybersecurity forums. Only in this way can effective actions be developed to address and overcome them.

[5] The United Nations Institute for Disarmament Research. (2019). *"Gender in Cyber Diplomacy Factsheet".* Available at: https://www.unidir.org/sites/default/files/2019-2/Gender%20in%20Cyber%20Diplomacy_Factsheet.pdf

Responses to Domestic Violence and Sexual Exploitation and Abuse

Latin America, MENA and West Africa

Newsletter N°3 / March 2021

Newsletter coordinator:

Barbara Shitnaan Maigari

Main Researchers:

Stephanie Wallace
Rodrigo Sánchez

Researchers

Elom Khaunbiow
ASSN – African Security Sector Network

Hala Salem
Al Quds Center for Political Studies

Janet Abubakkar
ASSN – African Security Sector Network

Rabha Allam
Al-Ahram Center for Political and Strategic Studies

General Coordination:

Samanta Kussrow

General advisory:

Marcela Donadio

Graphic design:

Rubén Longas

This newsletter was prepared by
GPSP Global Partnership for Security and Peace

Latin American Scurity and Defence Network https://www.resdal.org/ing/ https://www.facebook.com/resdal https://twitter.com/RESDAL_ secretaria@resdal.org