APC
ASOCIACIÓN PARA EL PROGRESO DE LAS COMUNICACIONES

MARCO PARA EL DESARROLLO DE UNA POLÍTICA DE CIBERSEGURIDAD QUE RESPONDA A LAS CUESTIONES DE GÉNERO

REVISIÓN DE LITERATURA

Marco para el desarrollo de una política de ciberseguridad que responda a las cuestiones de género: Revisión de literatura

Esta publicación fue desarrollada y producida por APC. La autora es la investigadora externa Paz Peña.

Coordinación y edición: Verónica Ferrari y Paula Martins (APC)

Apoyo editorial: Gaurav Jain (APC)

Corrección y revisión: Lori Nordstrom (APC)

Traducción: Clio E. Bugel

Diseño y compaginación: Cathy Chen (APC)

Publicado en 2023 por APC

ISBN 978-92-95113-61-9
APC-202306-GAPS-R-ES-DIGITAL-351

Esta publicación ha sido desarrollada con el apoyo del gobierno de Reino Unido.

I. INTRODUCCIÓN

Si bien es un hecho que los problemas de ciberseguridad se formulan en términos tecnofuncionales, y eso les otorga un halo de objetividad, la ciberseguridad es un campo muy cuestionado.[1] Como señala Deibert, el ciberespacio no tiene propiedades fijas en el tiempo y el espacio, lo que lo vuelve un campo inherentemente político: se trata de una competencia entre diferentes puntos de vista sobre el mundo, ideologías e intereses estratégicos, aunque todo ello se presente como si se tratara de supuestos incuestionables.[2] La seguridad, en tanto que valor, no es universal e inmutable; por el contrario, se apoya constantemente en prácticas socioculturales que caracterizan qué y a quién se considera "seguro/a" o "a salvo", y a qué o a quién se considera "inseguro/a", y se elabora a través de dichas prácticas, conceptualizando los objetos que se encuentran protegidos y articulando una justificación moral para dicha seguridad.[3] El abordaje de género, que ha sido adoptado por una serie de corrientes teóricas tales como los Estudios de ciencia, tecnología y sociedad (CTS), Interacción persona-ordenador (IPO), y la Agenda Mujeres, Paz y Seguridad (MPS), entre otras, ingresó al igual que las corrientes teóricas del feminismo y la interseccionalidad en la disputa acerca de qué es y cómo se entiende la ciberseguridad. Y aunque no existe un cuerpo teórico contundente que desarrolle la propuesta de la ciberseguridad desde estos marcos, este documento se propone explorar de qué manera se han incorporado estas perspectivas al campo de la ciberseguridad y cuáles son los elementos. Este documento forma parte de un abordaje desarrollado por la Asociación para el Progreso de las Comunicaciones (APC) para prestar apoyo a los y las responsables de la formulación de políticas y a las organizaciones de la sociedad civil brindándoles lineamientos prácticos para poder desarrollar políticas, leyes y estrategias de ciberseguridad que incluyan cuestiones de género. Por lo tanto, se espera que sea de utilidad para los múltiples grupos de interés en las contribuciones relativas a un enfoque de la ciberseguridad que incluya al género a fin de encontrar un marco teórico que sirva de base para sus políticas y sus acciones.

Este trabajo se organiza de la siguiente manera: primero, un breve planteo sobre conceptos importantes en torno del género. Segundo, una descripción del contexto general preexistente a la idea de que la ciberseguridad constituye un espacio de género. La tercera parte analiza las conexiones entre la irrupción de los derechos humanos en el concepto de ciberseguridad y la perspectiva de género, y examina los conceptos transversales más prevalentes en las diferentes investigaciones que aplican el género a las diversas áreas de la ciberseguridad. En la cuarta parte, hay un estudio más profundo de algunos de los tópicos en los que está más presente la perspectiva de género en ciberseguridad, para terminar, en la última parte, con un breve capítulo de conclusiones.

1. Nissenbaum, H. (2005). Where computer security meets national security. *Ethics and Information Technology, 7,* 61-73. https://doi.org/10.1007/s10676-005-4582-3; Deibert, R. (2018a). Trajectories for future cybersecurity research. In A. Gheciu & W. C. Wohlforth (Eds.), *The Oxford Handbook of International Security*; Slupska, J. (2019). Safe at Home: Towards a feminist critique of cybersecurity. St. Anthony's International Review, 15. https://ssrn.com/abstract=3429851
2. Deibert, R. (2018a). Op. cit.
3. Nissenbaum, H. (2005). Op. cit.

II. CONCEPTOS IMPORTANTES

Este examen de la literatura se basa en corrientes teóricas y de investigación diversas que no necesariamente aclaran cuál es su perspectiva sobre el feminismo y el enfoque de género – conceptos que, aunque relacionados entre sí, son ligeramente diferentes. Algunas corrientes utilizan los marcos de género y feminismo de manera indistinta; otras parecen referirse al análisis de género como uno de los niveles técnicos del feminismo; para otras, parece que el género no es más que un factor demográfico; y muchas responden al objetivo de hacer del género algo generalizado como estrategia para promover la igualdad de género en todas las esferas sociales. Al mismo tiempo, para algunas, el género sólo equivale a mujeres, mientras que otras son explícitas acerca de la diversidad de identidades que abarca ese concepto.

Debido a esta dificultad y teniendo en cuenta el objetivo general de examinar qué es lo que la ciberseguridad ha considerado que es el género hasta ahora, este trabajo no establece distinciones significativas entre esas nociones relacionadas. Sin embargo, se respetan los conceptos planteados al inicio (no se remplaza género por feminismo, por ejemplo) y sólo se establecen alertas cuando las consideraciones de género parecen alejarse de lo que llamamos análisis de género y feminismo. Pero, ¿qué significan esos conceptos? Parece importante realizar una elaboración conceptual muy general de las ideas que se repetirán en el texto.

Género: Conjunto de ideas, representaciones, prácticas y mandatos sociales elaborados en base a la diferencia anatómica entre los sexos. Pero el género es mucho más que un poderoso principio de diferenciación social: es un brutal productor de discriminación y desigualdades. Las ideas y prácticas de género jerarquizan a los seres humanos desde el punto de vista social, económico y legal.

Abordaje de género, o análisis de género: Herramienta para analizar las diferencias de género y mitigarlas. El género no consiste solamente en la diferencia entre los sexos, sino que también tiene que ver con el poder. Por lo tanto, un análisis convincente de género debe combinar el estudio sobre las diferencias y las cuestiones de poder. Este abordaje sólo puede tener una influencia analítica y estratégica en ciertas políticas públicas y acciones gubernamentales, pero no se propone generar nuevas perspectivas políticas.

Feminismo: El feminismo es un abordaje diverso e interdisciplinario sobre la cuestión de la igualdad y la equidad que se basa en el género, la expresión de género, la identidad de género, el sexo y la sexualidad, tal como se entiende entre las teorías de crítica social y el activismo político.

Incorporación de la perspectiva de género: El proceso de evaluación de las consecuencias de cualquier acción planificada – incluso legislaciones, políticas, o programas – para hombres y mujeres, en todas las áreas y a todo nivel. Su objetivo último es alcanzar la igualdad de género.

Perspectiva interseccional: La perspectiva interseccional identifica un sistema de diversas opresiones – entre las cuales está el género, pero también incluye la raza, la religión y la clase social, entre otras – que establecen la jerarquía de una persona en la sociedad, visibilizando otras diferencias que constituyen la identidad de las personas y enriqueciendo la noción de sujeto que, hasta el momento en el feminismo, sólo se percibía desde la perspectiva de su género. A partir de la interseccionalidad, surgen múltiples sujetos atravesados por diversos atributos. Así, los problemas sociales se han vuelto más complejos dado que el análisis incluye ahora múltiples sistemas de poder que hasta entonces se consideraban separados.[4]

4. Collins, P. (2019). *Intersectionality as Critical Social Theory*. Duke University Press.

III. CONTEXTO DE CIBERSEGURIDAD COMO UN ESPACIO DE GÉNERO

La cuestión de género en el área de la ciberseguridad ha estado ausente del diálogo y los debates sobre ciberseguridad porque aún hoy se considera un "asunto secundario".[5] Pero el mero hecho de no formar parte de las conversaciones no significa que no exista, o que la ciberseguridad sea neutra en cuanto al género. De hecho, las investigaciones muestran que la ciberseguridad, en su concepción más amplia, es un espacio donde el género existe y afecta el modo en que se concibe y despliega en los diferentes campos y estadios. Más específicamente, los estudios señalan que la lógica de la masculinidad hegemónica que se encuentra tanto en el campo de la seguridad, cuanto en el de la tecnología, tiene influencia sobre las prácticas de ciberseguridad.[6]

Por un lado, el campo de la seguridad se puede considerar una institución con características de género porque las diferencias de género están muy presentes, o son muy marcadas. Como señala Myrttinen, la seguridad "dura" y las actividades e instituciones relacionadas (por ejemplo, los militares) se consideran masculinas porque son ("verdaderos") hombres quienes las realizan y "sólo los hombres pueden hacerlas bien"."[7] En cambio, la seguridad "blanda" (por ejemplo, construir la paz, o brindar cuidados de salud) se asocia a lo femenino. Por lo tanto, su estructura, sus prácticas, valores, ritos y rituales reflejan nociones aceptadas de masculinidad y femineidad y, a su vez, se trata de una institución que ayuda a crear identidades de género.[8] En este contexto, la ciberseguridad sigue estando estrechamente relacionada con lo militar, de modo que los patrones de género tienden a repetirse en la ciberseguridad.[9]

Del mismo modo, las diferentes tradiciones del análisis feminista se propusieron desnaturalizar las relaciones con la tecnología en lo que se refiere al género. Se argumentaba que la representación simbólica de la tecnología tiene una fuerte influencia de género, a tal punto que la afinidad con la tecnología en las sociedades occidentales se considera hoy una parte integral y constitutiva tanto de la identidad de género masculina hegemónica, como de la cultura de la tecnología, lo que termina creando un círculo vicioso a raíz del cual hay más hombres trabajando en ese campo, de manera que son ellos los que producen más tecnología.[10] Más allá del contexto específico de la ciberseguridad, el diseño de la tecnología también responde a cuestiones de género: mal-construye, omite y consolida usos de género específicos y prácticas privilegiadas que se perciben como masculinas más que femeninas, además de crear estereotipos de femineidad bastante problemáticos.[11] Estos aspectos de la cuestión de género tienen un impacto directo en la ciberseguridad.

5. Pytlak, A. (2021). Bringing gender analysis into international cybersecurity. *Cyber Peace & Security Monitor, 1*(8). https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.8.pdf; Sharland, L., et al. (2021). *System Update: Towards a Women, Peace and Cybersecurity Agenda*. UNIDIR. https://doi.org/10.37559/GEN/2021/03; Shoker, S. (2021). *Making gender visible in digital ICTs and international security*. Report submitted to Global Affairs Canada. https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/research-canada-1.pdf
6. Nieminen, L. (2021). *Why is human trafficking excluded from the EU's cybersecurity?: An explorative study about cybersecurity and human trafficking in the European Union*. http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-9698
7. Myrttinen, H. (2020). *Tool 1: Security Sector Governance, Security Sector Reform and Gender*. DCAF, OSCE/ODIHR & UN Women. https://www.dcaf.ch/tool-1-security-sector-governance-security-sector-reform-and-gender
8. Barrett, F. J. (1996). The Organizational Construction of Hegemonic Masculinity: The Case of the US Navy. *Gender, Work & Organisation, 3*(3), 129-142. https://doi.org/10.1111/j.1468-0432.1996.tb00054.x
9. D'Hondt, K. (2016). *Women and Cybersecurity*. Master's thesis, Harvard Kennedy School. Nieminen, L. (2021). Op. cit.
10. Wajcman, J. (2000). Reflections on Gender and Technology Studies: In What State is the Art? *Social Studies of Science, 30*(3), 447-464. https://doi.org/10.1177/030631200030003005
11. Millar, K., Shires, J., & Tropina, T. (2021). *Gender approaches to cybersecurity: Design, defence and response*. United Nations Institute for Disarmament Research. https://doi.org/10.37559/GEN/21/01

IV. CONCEPTOS DE CIBERSEGURIDAD: TENSIONES DESDE UNA PERSPECTIVA DE GÉNERO

Para Dunn Cavelty, hay dos formas diferentes de entender las cibertecnologías que prevalecen en la sociedad. La primera considera que la ciberseguridad es una práctica consistente en reparar objetos rotos y la segunda cree que se trata de una herramienta para promover objetivos políticos.[12] En la concepción de Reid y van Niekerk,[13] pasamos de un abordaje de seguridad de la información (cuyo objetivo es proteger los sistemas y las redes informáticas existentes de acciones hostiles en un contexto exclusivamente organizacional) a un enfoque más amplio, que responde mejor a la masificación del uso de las tecnologías digitales. En ciberseguridad, se considera que las tecnologías generan debilidades que pueden tener consecuencias negativas en la sociedad, de forma que aparecen actores "peligrosos" y se establece un vínculo con la noción abstracta de "seguridad nacional". Los Estados son los actores a los que se convoca para restablecer el control sobre el mal uso de las cibertecnologías mediante un esfuerzo más coordinado y enfocado por parte de la sociedad a nivel nacional e internacional, los gobiernos y el sector privado. En este contexto, el ciberespacio se define como un entorno complejo que resulta de la interacción entre personas, software y servicios en internet a través de dispositivos tecnológicos y redes conectadas a internet. Así, la ciberseguridad implica proteger los intereses de una persona, una sociedad o una nación, incluyendo los bienes informáticos y no informáticos que deben protegerse de los riesgos relativos a su interacción con el ciberespacio.[14]

Pero cuando se trata de definir cuál es el "objeto referente" de la seguridad surgen tensiones y controversias para establecer qué es ciberseguridad.[15] La perspectiva de ciberseguridad con enfoque de género se basa en una mirada centrada en lo humano. Esta estrategia, en lugar de priorizar la soberanía territorial de las redes, coloca a los seres humanos – sin importar su nacionalidad, o su lugar de residencia – como el principal objeto de seguridad y las redes se consideran una base esencial para el ejercicio contemporáneo de derechos humanos tales como el acceso a la información, la libertad de pensamiento y la libertad de asociación.[16] Este abordaje difiere de aquéllos basados en la seguridad nacional, para los cuales el Estado, las infraestructuras y las instituciones constituyen el foco de las amenazas de ciberseguridad. También difiere de los enfoques del sector privado, para los cuales los seres humanos se reducen a nodos de la red necesarios para aumentar el rédito.[17]

12. Dunn Cavelty, M. (2018). Cybersecurity Research Meets Science and Technology Studies. *Politics and Governance,* 6(2), 22-30. https://www.cogitatiopress.com/politicsandgovernance/article/download/1385/1385
13. Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. *Information Security for South Africa 2014*. https://ieeexplore.ieee.org/document/6950492
14. Ibid.; Slupska, J. (2019). Op. cit.
15. Slupska, J. (2019). Op. cit.; Dunn Cavelty, M. (2014). Op. cit.; Brown, D., & Esterhuysen, A. (2019, 28 November). Why cybersecurity is a human rights issue, and it is time to start treating it like one. *APC*. https://www.apc.org/en/node/35879
16. Deibert, R. (2018b). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs, 32*(4), 411-424. https://doi.org/10.1017/S0892679418000618
17. Kumar, S. (2021). The missing piece in human-centric approaches to cybernorms implementation: The role of civil society. *Journal of Cyber Policy, 6*(3), 375-393. https://doi.org/10.1080/23738871.2021.1909090

El diálogo sobre el abordaje de la ciberseguridad centrada en lo humano destaca la importancia de los estándares internacionales sobre derechos humanos como base y marco para la ciberseguridad. Existe un consenso en cuanto a la aplicación completa e indiscriminada de las normas del derecho internacional al ciberespacio. Sin embargo, algunos derechos son particularmente relevantes en el ciberespacio por encontrarse directamente vinculados a la información en sus diversos aspectos y manifestaciones. Por ejemplo, la privacidad y la libertad de expresión e información complementan al derecho a la seguridad, la libertad personal y la no discriminación.[18] Así, el peligro de la "ciber inseguridad" nunca debería constituir un pretexto para violar los derechos humanos, cuya protección debería constituir el núcleo de toda política de ciberseguridad.[19]

En este contexto, la pregunta que se hace desde el enfoque de género es hasta qué punto la ciberseguridad presupone los sistemas de poder que jerarquizan socialmente a los seres humanos, tanto en cuanto al diseño de estrategias, como a los efectos de los ataques. En este sentido, la "ciberseguridad feminista", como la llama Slupska,[20] constituye un abordaje cuestionador: ¿para quién están hechas esas tecnologías? ¿dónde se puede intervenir? ¿qué es lo que se negocia en las empresas de tecnología cuando surgen dificultades? ¿de quién es esta ciberseguridad? Sin embargo, aunque estas preguntas se han multiplicado en los últimos años, aún no hay una elaboración conceptual completa, o consensuada, de cuáles son los elementos que debería incluir una definición de ciberseguridad desde la perspectiva de género. De todas formas, podemos mencionar algunos conceptos importantes que destacan diferentes autores.

Primero, se cuestiona la supuesta neutralidad del ciberespacio, que supone que los seres humanos son una entidad universal neutra ya que, como denuncian las corrientes teóricas feministas, en una realidad heteropatriarcal y colonial, el ser humano siempre termina siendo un hombre blanco cis heterosexual. Por un lado, este cuestionamiento afecta la esfera de los peligros de las personas y la forma en que los sistemas y políticas de ciberseguridad entienden esos peligros diferenciados. Las comunidades de activistas por los derechos humanos, periodistas y personas en situación de marginalidad o vulnerabilidad debido a su religión, etnicidad, orientación sexual, o identidad de género, por ejemplo, pueden estar sujetas a ciertos riesgos especiales y sufrir las consecuencias de algunas amenazas específicas.[21] Como dicen Haciyakupoglu y Wong, el supuesto de que el ciberespacio es neutro en términos de género pasa por alto las diferencias de capacidades, necesidades y prioridades de los diferentes géneros y la forma en que la normativa de género condiciona las prioridades dentro de los diseños de ciberseguridad, donde los sistemas suelen modelarse en base al usuario hombre promedio.[22]

Como consecuencia del punto anterior, resulta de vital importancia para la perspectiva de género en ciberseguridad que se denuncie la carencia de diversidad tanto en el desarrollo de tecnologías, como en el diseño de estrategias y políticas de ciberseguridad. En este sentido, una parte importante del enfoque

18. Álvarez, D., & Vera, F. (2017). Ciberseguridad y derechos humanos en América Latina. In A. del Campo (Ed.), *Hacia una internet libre de censura II: Perspectivas en América Latina*. Universidad de Palermo. https://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf
19. Brown, D., & Esterhuysen, A. (2019, 28 November). Op. cit.
20. Slupska, J. (2019). Op. cit.
21. Brown, D., & Esterhuysen, A. (2019, 28 November). Op. cit.
22. Haciyakupoglu, G., & Wong, Y. (2021). *Gender, Security and Digital Space: Issues, Policies, and the Way Forward*. S. Rajaratnam School of International Studies. https://www.rsis.edu.sg/rsis-publication/cens/gender-security-and-digital-space-issues-policies-and-the-way-forward

feminista de la ciberseguridad entiende que la producción de conocimiento sobre tecnologías y ciberseguridad está inevitablemente ligada a actos de poder y supone que, en las sociedades patriarcales donde la epistemología científica occidental ha sido universalizada, se suprime el conocimiento de las mujeres.[23] Más aún, sobre todo en el área de la ciberseguridad, la experiencia técnica suele asociarse a los hombres y la masculinidad.[24] En este sentido, el llamado a la diversidad tiene que ver con la inspiración de la epistemología feminista del punto de vista, que promueve la reevaluación de las experiencias de las mujeres como epistemologías alternativas válidas para la ciberseguridad.[25] Esto implica problematizar la falta de diversidad interseccional en el sentido más amplio: desde la ausencia de personas diversas que trabajen en la industria y el desarrollo de políticas, hasta la necesidad de contar con una mirada crítica de las metodologías que subyacen a la ciberseguridad.

Así, por un lado, se revisan de manera crítica los modelos de ciberseguridad que persisten en el uso de metodologías que adolecen de prejuicios de género y brechas de conocimiento. Según Julia Slupska, un abordaje feminista de la ciberseguridad debe enraizarse poniendo el foco en el daño que genera a los humanos.[26] Además, a la hora de analizar el daño potencial que implican los ciberataques para las personas, el desafío consiste en dejar atrás la división "público versus privado" que establecía la corriente tradicional de la ciberseguridad, enfocada en la seguridad nacional. Es necesario enfocarse, en cambio, en los impactos a nivel micro[27] tales como el espacio doméstico y el privado, ya que éste último no puede entenderse sólo como un espacio de seguridad amenazado por adversarios externos.[28] Esto lleva a descartar cierto elitismo de la ciberseguridad tradicional, especialmente cuando la comunidad de usuarios y usuarias de tecnología se consideran meramente como "el factor humano", lo que los/as vuelve invisibles, y permite enfocarse en actores más poderosos, tales como empresas, Estados, o ejércitos.[29] Sin embargo, la única manera de saber cuáles son los diversos peligros que pueden afectar a la gente es renovar las prácticas de elaboración de modelos de amenaza y rever cómo se relacionan con la ciberseguridad como concepto y como práctica.[30] En otras palabras, es necesario hacer un diseño de seguridad participativa, ya que ello impide suponer que la seguridad de cada individuo se deriva de la seguridad de un sistema técnico e incluye la perspectiva de actores que, en general, podrían ser marginados.[31] Esto es lo que caracteriza a una tendencia de pensamiento

23. Bardzell, S. (2010). Feminist HCI: Taking stock and outlining an agenda for design. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. https://doi.org/10.1145/1753326.1753521
24. Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.
25. Slupska, J., Dawson Duckworth. S., Ma, L., & Neff, G. (2021). Participatory threat modelling: Exploring paths to reconfigure cybersecurity. *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3411763.3451731
26. Slupska, J. (2019). Op. cit.
27. Tickner, J. A. (2004). Feminist responses to international security studies. *Peace Review, 16*(1), 43-48. https://doi.org/10.1080/10402650420002101 48
28. Slupska, J. (2019). Op. cit.
29. Still, an important caveat must be made: calls for the inclusion of domestic and private spaces into cybersecurity frameworks must be careful to justify unwanted intrusions into the lives of minority and lower-class populations since, traditionally, these are the most vulnerable to constant state interventions. See: Slupska, J. (2019). Op. cit.
30. Slupska, J., Dawson Duckworth, S., Neff, G., et al. (2021). *Reconfigure: Feminist Action Research in Cybersecurity*. Reconfigure Network. https://www.oii.ox.ac.uk/news-events/news/reconfigure-feminist-action-research-in-cybersecurity
31. Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019). Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. *Proceedings of the New Security Paradigms Workshop (NSPW '19)*. https://doi.org/10.1145/3368860.3368861; Slupska, J., Dawson Duckworth, S., Ma, L., & Neff, G. (2021). Op. cit.

distinto sobre la ciberseguridad según el cual las personas dejan de ser consideradas como una dimensión problemática, y por tanto, excluida, y pasan a ser parte de la solución, ya que se reconoce el potencial que tienen para contribuir al éxito de la ciberseguridad dentro del sistema sociotécnico, que es más amplio.[32]

Los desafíos no acaban aquí, porque una vez que la ciberseguridad se analiza a nivel micro, es decir, los espacios de seguridad personal, resulta esencial volver a elaborar metodologías de educación en ciberseguridad. Hoy en día se utiliza mucha jerga técnica y se recurre a la culpabilización de las víctimas, es decir, se responzabiliza a usuarios y usuarias por elegir claves débiles, por cliquear enlaces de phishing, o por compartir imágenes de desnudos.[33] Es más, metodologías tales como la "seguridad holística", ampliamente utilizadas por expertos en seguridad digital en el campo de los derechos humanos, tienen por objetivo alejarse de la máquina y aproximarse a prácticas feministas de cuidado y autocuidado. Este abordaje rechaza la tradición de seguridad militarizada y propone una definición de seguridad – "bienestar en acción" – basada en el cuidado, en la que cuidado significa rechazar el temor a peligros abstractos y adoptar en cambio lo que es inminente y significativo para las personas y su propio cuerpo.[34] Además, la educación no debería enfocarse solamente en las personas potencialmente receptoras de ataques digitales ya que esto, según Slupska, las hace responsables de evitar la mala utilización:

> La educación también debería abarcar a los abusadores y a quienes venden herramientas para cometer abusos, que son los principales responsables de los daños que causan esas herramientas. Si bien es probable que muchos proveedores y clientes de las herramientas para cometer abusos no cambien de opinión, es posible que algunos se den cuenta de que sus acciones son antiéticas debido a un entorno social que acepta las prácticas de vigilancia. Se podrían incorporar a la ética digital los principios feministas del consentimiento y el respeto de la autonomía, y enseñarse desde una temprana edad.[35]

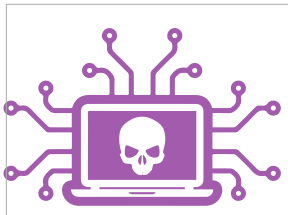
32. Zimmermann, V., & Renaud, K. (2019). Moving from a "human-as-problem" to a "human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies, 131*, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005
33. Slupska, J., Dawson Duckworth, S., Neff, G., et al. (2021). Op. cit.
34. Kazansky, B. (2021). 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. *Big Data & Society, 8*(1). https://doi.org/10.1177/2053951720985557
35. Slupska, J. (2019). Op. cit.

V. NODOS CLAVES DE CIBERSEGURIDAD PARA UNA PERSPECTIVA DE GÉNERO

En la sección siguiente, identificamos nodos específicos de ciberseguridad que la investigación de género analiza en forma crítica. Los conceptos transversales que examinamos antes también se desarrollan en todos esos nodos. Como se verá, todos los nodos se relacionan entre sí, de modo que esta clasificación – y, por lo tanto, su separación – sólo apunta a ordenar referencialmente los cuerpos de investigación y una serie de pruebas más robustas.

A) La brecha de género en el campo de la ciberseguridad

B) Las dimensiones de la violencia de género en ciberseguridad



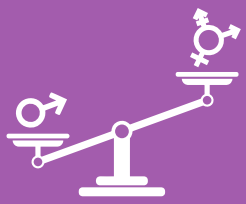
C) Vulnerabilidad diferencial ante ciberataques

D) Impacto diferenciado de ciberincidentes según el género

E) Reconfigurar los marcos de análisis de la ciberseguridad

F) Infraestructura de una internet autónoma y feminista

G) Políticas públicas internacionales de ciberseguridad



A) LA BRECHA DE GÉNERO EN EL CAMPO DE LA CIBERSEGURIDAD

Existe un consenso generalizado en cuanto a que, desde hace ya algunos años y debido a la digitalización y el aumento de los ciberataques, la industria de la ciberseguridad mundial sufre una gran carencia de trabajadores/as capacitados/as. La brecha actual que hay en la fuerza de trabajo en ciberseguridad es de más de 3,1 millones de profesionales especializados/as a nivel mundial y si bien el número de profesionales de la industria tuvo un aumento de más de 700 mil personas en 2020, las mujeres siguen representando apenas 25% de la fuerza total de trabajo en ciberseguridad, mientras que constituyen al menos 40% del total de la fuerza de trabajo global, según el Pew Research Center.[36]

Este problema se ha analizado hasta ahora desde dos perspectivas: la industria y la participación en políticas relativas a la ciberseguridad. Del mismo modo, resulta necesario subrayar que, si bien la base del problema parece ser la falta de participación de las mujeres en esos espacios, se va notando cada vez más que, por un lado, no todas las mujeres sufren esta discriminación de la misma forma y es esencial realizar otros cruzamientos interseccionales en el análisis y, por otro lado, la crisis de diversidad va más allá de la participación sólo de las mujeres, ya que otros grupos históricamente discriminados siguen siendo excluidos.

Diversidad en la industria

Un estudio global cualitativo de (ISC)², publicado en 2021, concluyó que hay una percepción muy extendida de que el grupo de profesionales de la industria de la ciberseguridad tiene un perfil muy homogéneo: hombres blancos de mediana edad con más de ocho años de experiencia en el campo de las TI, o relacionado con la informática.[37] Además, se identifica dos problema estructurales en que afectan aún más a la industria: por un lado, la incorporación de mujeres jóvenes es muy lenta, y por otro lado, la ausencia de diversidad es muy notoria en los cargos directivos. Esta falta de diversidad en los equipos de ciberseguridad se vuelve un círculo vicioso, ya que hace que las condiciones de trabajo en ciberseguridad sean aún más difíciles para las mujeres. Por ejemplo, Barsh y Yee destacan la relación existente entre el grado de diversidad en una organización y la probabilidad de que las mujeres sean promovidas a cargos directivos.[38] Del mismo modo, el intenso horario de trabajo en la cultura masculinizada de la

36. (ISC)². (2021). *In Their Own Words: Women and People of Color Detail Experiences Working in Cybersecurity.* https://www.isc2.org/-/media/ISC2/DEI/DEI-Market-Research-2021.ashx
37. Ibid.
38. Barsh, J., & Yee, L. (2011). *Unlocking the full potential of women in the US economy*. McKinsey & Company.

ciberseguridad constituye un modelo impráctico para las personas que tienen la responsabilidad de brindar cuidados (y es más probable que éstas sean mujeres).[39] Además, el abuso y el acoso, así como el ciberacoso, son problemas muy extendidos, como lo muestra un estudio reciente de Respect in Security, en el cual se calcula que alrededor de un tercio del grupo de profesionales de la ciberseguridad tuvo experiencias personales de acoso y abuso en línea (32%) y en persona (35%).[40]

Otro problema es la ausencia de diversidad relacionada con la experiencia y las capacidades de las personas.[41] O sea, la escasa diversidad se refiere no sólo al género, la raza y la religión, sino también a la creación de equipos con una variedad de experiencias que puedan generar una cultura pluralista y abordajes innovadores para la solución de problemas, ya que los adversarios aprovecharán los prejuicios inconscientes arraigados en la industria reconociendo y esquivando la homogeneidad de los enfoques típicos sobre seguridad.[42] King-Close sostiene que, dado que la ciberseguridad es un nuevo dominio de batalla que requiere nuevas perspectivas para la solución de problemas, algunos de los obstáculos que alejan a las mujeres y a otros grupos de la guerra – y roles relacionados con la tecnología – se pueden superar.[43] Una indicación de ello es, por ejemplo, la creciente necesidad de incorporar la psicología al análisis de la ciberseguridad, lo que además puede significar una oportunidad para aumentar la diversidad ya que se trata de una carrera tradicionalmente feminizada. Sin embargo, por el momento no vale la pena realizar estudios fuera del área de ciencias, tecnología, ingeniería y matemática (STEM, en inglés) para trabajar en ciberseguridad, ya que la mayoría de los empleadores consideran prioritaria la formación en ciencias informáticas o ingeniería.[44]

Entre las respuestas posibles a este problema, a nivel educativo, cada vez hay más evidencia de la necesidad de adoptar una mirada interseccional para analizar la lenta incorporación de las mujeres al área de la ciberseguridad, sobre todo en lo que se refiere a sus experiencias de educación en STEM cuando el género se cruza con la raza y la etnicidad.[45] Además, a nivel profesional, la industria está adoptando cada vez más las metodologías DEI (diversidad, equidad e inclusión) para incrementar la diversidad dentro de la profesión de la ciberseguridad, creando así espacio para el respeto de las diferencias biológicas, demográficas, o culturales, además de las diferentes maneras de pensar, experiencias, capacidades, o estilos de liderazgo.[46]

Diversidad en la gobernanza

El género es una condicionante esencial de los riesgos que corre la seguridad de las mujeres, los hombres y las personas de diferentes identidades de género y expresiones en línea, y también determina el grado de seguridad – o no – con

39. D'Hondt, K. (2016). Op. cit.; Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.
40. Respect in Security. (2021, 21 July). Over a third of cybersecurity professionals have experienced harassment at industry events. https://respectinsecurity.org/respect-in-security-press-release
41. (ISC)². (2021). Op. cit.
42. Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2019). Educating Future Multidisciplinary Cybersecurity Teams. *Computer, 52*(3), 58-6. https://doi.org/10.1109/MC.2018.2884190
43. King-Close, A. M. (2016). *A gender analysis of cyber war*. Tesis de Maestría, Escuela de extensión de Harvard.
44. Poster, W. R. (2018, 26 March). Cybersecurity needs women. *Nature*. https://www.nature.com/articles/d41586-018-03327-w
45. Burrell, D. (2018). An exploration of the cybersecurity workforce shortage. *International Journal of Hyperconnectivity and the Internet of Things, 2*(1). http://dx.doi.org/10.4018/IJHIoT.2018010103
46. (ISC)². (2021). Op. cit.

el que pueden acceder a los espacios en línea y usarlos. Por lo tanto, se vuelve imperativo resolver la falta de participación de las mujeres y las personas con identidades de género diversas en la ciberseguridad y la gobernanza de la misma incorporando una perspectiva de género a la vigilancia, la prestación y la gestión de la ciberseguridad.[47] Pero, según Brown y Pytlak, la participación de las mujeres que trabajan en políticas y diplomacia de ciberseguridad se ha estudiado mucho menos que la falta de diversidad en la industria, tanto en sus dimensiones cuantitativa como cualitativa.[48] Por ejemplo, un análisis de las negociaciones sobre ciberseguridad internacional realizado por el Instituto de las Naciones Unidas de Investigación sobre el Desarme (UNIDIR) reveló que sólo una de cada cinco participantes es mujer y cuando los Estados enviaron un/a único/a representante, se trató casi invariablemente de un hombre.[49]

La participación de las mujeres en la toma de decisiones sobre ciberseguridad a nivel internacional es importante no sólo como forma concreta de reducir la desigualdad de género, sino también para incluir una diversidad de perspectivas que pueden servir para tratar la información con más cuidado y tomar mejores decisiones políticas que incluyan las necesidades específicas que tienen las mujeres en el área de la ciberseguridad.[50] En su investigación, Brown y Pytlak revelan que los roles patriarcales asignados culturalmente inciden de varias maneras sobre la experiencia de las mujeres en ciberpolíticas: desde la falta de participación, hasta el debilitamiento constante de su liderazgo político.[51] Además, como es habitual en la sociedad, las tareas de cuidado que suelen recaer en las mujeres también son un factor de discriminación. Sin embargo, para estas investigadoras, el problema de la diversidad de género no constituye una realidad únicamente "cibernética", sino un problema social más amplio que se manifiesta como inequidad de género en los espacios de ciberseguridad, de modo que la solución implica cambios culturales más generales y abarcadores.

47. Dorokhova, E., vale, h., Laçí, V., & Mahmutovic, A. (2021). *Cyber violence against women and girls in the Western Balkans: Selected case studies and a cybersecurity governance approach*. Centro de Ginebra para la Gobernanza del Sector de la Seguridad (DCAF). https://www.dcaf.ch/sites/default/files/publications/documents/CyberVAWG_in_WB.pdf
48. Brown, D., & Pytlak, A. (2020). *Why Gender Matters in International Cyber Security*. Liga Internacional de Mujeres por la Paz y la Libertad y Asociación para el Progreso de las Comunicaciones. https://www.apc.org/en/pubs/why-gender-matters-international-cyber-security
49. UNIDIR. (2021). *Fact sheet: Gender in cyber diplomacy*. https://unidir.org/publication/fact-sheet-gender-cyber-diplomacy
50. Sharland, L., et al. (2021). Op. cit.
51. Brown, D., & Pytlak, A. (2020). Op. cit.

B) LAS DIMENSIONES DE LA VIOLENCIA DE GÉNERO EN CIBERSEGURIDAD

Buena parte de la investigación sobre género y ciberseguridad procede de estudios sobre violencia y desigualdad de género en el sector de las tecnologías digitales.[52] Las mujeres y las niñas se ven enfrentadas a un tipo de ciberamenazas específicas en la era digital. Dichas amenazas se consideran formas de la violencia de género, porque ocurren debido a su género, o porque afectan a uno solo de los géneros de manera desproporcionada. Aunque esta violencia ocurre a través de las tecnologías digitales, forma parte de la misma violencia estructural que existe fuera de línea, pero su dimensión tecnológica agrega elementos de búsqueda, persistencia, replicabilidad y adaptabilidad que ayudan a los agresores a tener acceso a sus blancos y pueden exacerbar el daño. La violencia de género en línea se puede manifestar de varias formas, pero lo que prevalece es la violación de la privacidad como arma de los agresores. Así, por ejemplo, como señala la Relatora Especial de Naciones Unidas sobre la violencia contra la mujer en un informe, existen ataques tales como el acceso no consensuado, el uso, la manipulación, difusión o intercambio de datos, información y/o contenido, fotografías y/o videos privados, incluyendo imágenes, audio y/o videoclips, o imágenes "fotoshopeadas" sexualizadas.[53] A pesar de ser un tipo de violencia creciente que tiene consecuencias materiales, psicológicas y económicas para las mujeres y la sociedad, la violencia de género en línea suele no considerarse un problema de ciberseguridad debido a la subestimación de asuntos domésticos/privados y porque se elige dar prioridad a las amenazas más graves.[54] Este desinterés tiene consecuencias directas para las mujeres y las niñas ya que, además de la violencia de género en línea, también ignora la violencia íntima facilitada por la tecnología, la violencia de género política en línea y el componente de violencia de género de la radicalización terrorista en internet.

El abuso, facilitado por la tecnología, por parte de compañeros íntimos (también conocido como abuso por parte de compañero íntimo, IPA por su sigla en inglés) tiene una diferencia significativa con otros tipos de violencia de género en línea, sobre todo porque los agresores y los/as sobrevivientes no son alguien desconocido. De hecho, están o han estado involucrados/as en una relación íntima que incluye una convivencia diaria tanto en línea, como fuera de línea. Esto significa que los agresores no sólo tienen acceso a las víctimas y sus dispositivos en el mundo físico, sino que también pueden conocerlos/as

52. Ibid.
53. Šimonović, D. (2018). *Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos*. A/HRC/38/47. https://undocs.org/A/HRC/38/47
54. Slupska, J. (2019). Op. cit.

de manera íntima, al igual que conocen sus rutinas, sus hábitos y sus preferencias.[55] Influidos/as sobre todo por Interacción persona-ordenador (HCI), numerosos/as autores/as empezaron a investigar el papel que pueden tener las tecnologías digitales en las relaciones abusivas[56] y, más específicamente, el rol de la "internet de las cosas" y su relación con el abuso por parte de un compañero íntimo y la seguridad. Las características de las tecnologías digitales, incluso asuntos tales como los ajustes de uso, se pueden utilizar mal para abrir grietas por las cuales la persona perpetradora de violencia doméstica y violencia por parte de un compañero íntimo puede llevar a cabo el "tecno-abuso", o sea, vigilar, coaccionar, o controlar a la otra persona, de manera que la seguridad de los dispositivos es crucial para los grupos y comunidades que se encuentran en relaciones vulnerables.[57] Del mismo modo, y a pesar de su prevalencia en la sociedad, el abuso por parte de un compañero íntimo es algo que se ignora por completo en las investigaciones que analizan la seguridad de los dispositivos inteligentes del hogar. El diseño de esos dispositivos "supone, en general, que el/la 'propietario/a' del dispositivo no constituye una amenaza para los/as demás usuarios/as del dispositivo. Esta omisión refleja algo que las teorías feministas critican desde hace tiempo y es el concepto binario interno/externo, según el cual el hogar se piensa como un lugar de seguridad y protección contra la amenaza de adversarios externos."[58]

Del mismo modo, y aunque la violencia de género a través de las TIC suele quedar fuera de los límites legales de la guerra, las TIC se pueden pensar como herramientas que perturban la vida política a través de la violencia de género pero, al igual que en muchas otras áreas de la política, falta la recolección sistemática de datos sobre estos ataques, tanto durante, como por fuera de las transiciones de gobierno.[59] En este aspecto, en su informe específico de 2018 sobre violencia contra las mujeres en política,[60] la Relatora Especial de Naciones Unidas sobre la violencia contra las mujeres identifica la desinformación de los actores estatales y no estatales como una forma de la violencia de género en línea:

> En definitiva, la violencia en línea contra las mujeres en política constituye un ataque directo contra la participación plena de las mujeres en la vida política y pública, y contra el ejercicio de sus derechos humanos. Aún no queda del todo claro hasta qué punto los actores estatales y no estatales utilizan esa violencia en línea para propagar la desinformación que apunta a desalentar a las mujeres de participar en política, barriendo el apoyo popular a las mujeres políticamente activas e influyendo en la manera que tienen los hombres y las mujeres de ver algunos puntos en particular.[61]

55. Leitao, R. (2019). Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. *DIS '19: Proceedings of the 2019 on Designing Interactive Systems Conference*. https://doi.org/10.1145/3322276.3322366
56. Harris, B. A., & Woodlock, D. (2019). Digital Coercive Control: Insights from two landmark domestic violence studies. *The British Journal of Criminology, 59*(3), 530-550. https://doi.org/10.1093/bjc/azy052; Leitao, R. (2019). Op. cit.; Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019). Op. cit.; Slupska, J. (2019). Op. cit.; Slupska, J., & Tanczer, L. M. (2021). Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. In J. Bailey, A. Flynn & N. Henry (Eds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211049
57. Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019). Op. cit.
58. Slupska, J. (2019). Op. cit.
59. Shoker, S. (2021). Op. cit.
60. Šimonović, D. (2018). *Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias sobre la violencia contra la mujer en la política*. A/73/301. https://undocs.org/A/73/301
61. Entre las razones que hay para considerar a la desinformación como una amenaza para la ciberseguridad está el hecho de que la manipulación de los datos incide y manipula, a su vez, los temores y las emociones de las personas, comprometiendo así la seguridad de la información y utilizando la ciberinfraestructura. Ver: EU Disinfo Lab. (2021, 24 May). Why Disinformation is a Cybersecurity Threat. https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat

Según Di Meco, la desinformación de género se puede definir como la difusión de información e imágenes engañosas, o inapropiadas, de las mujeres que son líderes en política, periodistas y figuras públicas. Esa desinformación suele enmarcarse en líneas argumentales misóginas y estereotipos de género relativos al rol de las mujeres.[62] Este tipo de desinformación está diseñado para alterar la percepción pública de la trayectoria de las mujeres dedicadas a la política a fin de obtener un rédito político inmediato, además de desalentar a las mujeres de la carrera política. Puede proceder de adversarios políticos domésticos o internos (incluso de actores estatales), o ser resultado de una interferencia externa o extranjera, en cuyo caso merece ser objeto de atención específica a causa de su naturaleza, volumen e impacto en los procesos democráticos.

En este contexto, hay evidencia de falta de información de género por parte del Estado por la cual, actores que forman parte de un Estado o cuya conducta, o intereses se alinean a un Estado, generan una desinformación de género para obtener resultados políticos.[63] Al mismo tiempo, también hay evidencia del empleo de tácticas de desinformación de género empleadas por actores de un Estado para debilitar las instituciones democráticas de otros países. Por ejemplo, una imagen de pantalla de un comentario falso de Facebook sobre la desnudez de Svitlana Zalishchuk, miembro del Parlamento de Ucrania, fue amplificada por varios sitios web rusos y luego compartida activamente por usuarios/as de las redes sociales ucranianas con el fin de desacreditarla políticamente y estropear su carrera política.[64]

Un fenómeno vinculado a la desinformación de género es la radicalización terrorista en internet. Existe un consenso en la literatura sobre violencia extremista en cuanto a que internet es un "acelerador" de la radicalización, ya que las ideas extremistas se normalizan dentro de una comunidad de individuos que se validan entre sí. Más aún, los/as expertos/as en masculinidades reconocen que los individuos que perpetúan la violencia política no estatal son mayoritariamente hombres, lo que constituye una característica común que se extiende por todo el espectro ideológico, y así se vuelve más probable que los grupos políticamente violentos los identifiquen y los recluten.[65] En particular, algunas de esas comunidades en línea fueron responsables de perpetuar el ciberacoso a las mujeres, recurriendo principalmente a tácticas como el doxeo y las amenazas de violencia física y sexual contra las activistas feministas.[66] En este contexto, el análisis de género de las amenazas se vuelve necesario, ya que podría ayudar a entender los diferentes atractivos que ofrecen las diversas plataformas de internet para esos grupos. Así, se podría evaluar algunos de los riesgos que suponen para la paz y la seguridad.[67]

62. Di Meco, L. (2020). *Online Threats to Women's Political Participation and The Need for a Multi-Stakeholder, Cohesive Approach to Address Them*. UN Women. EGM/CSW/2021/EP8. https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/CSW/65/EGM/Di%20Meco_Online%20Threats_EP8_EGMCSW65.pdf
63. Judson, E., Atay, A., Krasodomski-Jones, A., & Smith, J. (2020). *Engendering hate: The contours of state-aligned gendered disinformation online.* Demos. https://apo.org.au/sites/default/files/resource-files/2020-10/apo-nid309184.pdf
64. Di Meco, L. (2019). *#SHEPERSISTED: Women, Politics & Power in the New Media World.* https://www.iknowpolitics.org/sites/default/files/191105shepersisted_final.pdf
65. Shoker, S. (2021). Op. cit.; Sharland, L., et al. (2021). Op. cit.
66. Shoker, S. (2021). Op. cit.
67. Sharland, L., et al. (2021). Op. cit.

C) VULNERABILIDAD DIFERENCIAL ANTE CIBERATAQUES

La noción de "vulnerabilidades diferenciales" de Pierce et al. revela que diferentes poblaciones e individuos tienen diferentes tipos y grados de vulnerabilidad en relación a la seguridad digital, y que pueden estar sujetos a una gran variedad de ataques.[68] Esta noción se basa en estudios feministas, queer y raciales sobre la vulnerabilidad, y por lo tanto contradice los discursos dominantes sobre seguridad técnica que enmarcan la seguridad como un valor objetivo, o universal, y consideran al/a "usuario/a inseguro/a" como un estado objetivo. Este concepto, a su vez, elude la expresión "poblaciones vulnerables", que puede estigmatizar y desempoderar a los individuos así etiquetados y construir una relación de poder en la que investigadores/as, ingenieros/as y responsables de la formulación de políticas adoptan el papel de protectores/as, lo que puede contribuir a reafirmar relaciones de poder no equitativas. Según esta lógica, la vulnerabilidad diferencial conlleva una segunda noción relacionada con la primera – la de confianza diferencial – según la cual quién confía en quién y con qué propósito es algo que depende principalmente de qué usuarios/as necesitan protección y de cuál es su posición dentro de grupos y contextos sociales particulares. En este contexto, las vulnerabilidades diferenciales atribuidas al género han tenido una prominencia considerable incluso en el campo de la ciberseguridad tradicional, como veremos.

En general, hasta ahora han existido dos maneras dominantes de reflexionar sobre las varias vulnerabilidades diferenciales basadas en el género.

Acceso a internet y conocimiento digital

Los datos globales más recientes de la Unión Internacional de Telecomunicaciones (UIT)[69] muestran que, en promedio, 62% de los hombres utiliza internet en todo el planeta, mientras que las mujeres constituyen sólo 57%. Aunque la brecha digital de género se redujo en todas las regiones del mundo y casi desapareció en el mundo industrializado (89% de los hombres y 88% de las mujeres tiene conexión), sigue habiendo brechas significativas en los países menos industrializados (31% de los hombres, versus 19% de las mujeres) y en

68. Pierce, J., Fox, S., Merrill, N., & Wong, R. (2018). Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. *Proceedings of the ACM on Human-Computer Interaction, 2*. https://doi.org/10.1145/3274408
69. Unión Internacional de Telecomunicaciones. (2021). *Measuring digital development: Facts and figures 2021*. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

los países en desarrollo sin salida al mar (38% de los hombres, frente a 27% de las mujeres). Además, la brecha de género sigue siendo particularmente notable en África (35% de los hombres versus 24% de las mujeres) y en los Estados árabes (68% de los hombres versus 56% de las mujeres).

Sin embargo, la contínua reducción del precio de las conexiones de banda ancha y el costo de los dispositivos no impide que las personas, una vez conectadas, carezcan de los conocimientos necesarios para aprovechar esta tecnología a fin de mejorar su vida. Más aún, según EQUALS y UNESCO, existe amplia evidencia de la gravedad de la brecha de género actual en relación a los conocimientos digitales: en términos globales, es menos probable que las mujeres sepan utilizar un teléfono inteligente, navegar en internet, utilizar redes sociales y entender cómo salvaguardar la información en los medios digitales.[70] Más aún, los estudios etnográficos realizados en países y comunidades destacan el hecho de que las culturas patriarcales suelen impedir que las mujeres y las niñas desarrollen sus capacidades digitales. Y, lo que es aún más preocupante, las brechas digitales en el área de las capacidades digitales parecen aumentar a medida que las tecnologías se vuelven más sofisticadas y costosas, a pesar de las intervenciones realizadas durante al menos dos décadas para promover la igualdad de género.

La carencia de habilidades digitales de las mujeres las sitúa en una posición de particular vulnerabilidad en lo que se refiere a la gestión de su ciberseguridad. Como se vio en el informe especial de EQUALS y UNESCO sobre la brecha de género en el área de las habilidades digitales,[71] en muchos contextos, las mujeres y las niñas deben enfrentarse al riesgo de violencia física si poseen, o piden prestados dispositivos digitales, lo que en algunos casos implica que los usan en secreto, con lo cual se vuelven más vulnerables a las amenazas en línea y además, con dispositivos prestados es aún más difícil que adquieran conocimientos digitales. Además, las mujeres que están fuera de línea se encuentran especialmente en riesgo si se ven expuestas a amenazas vacías y esquemas de suplantación de identidad que son comunes en el mundo digital. Las mujeres que carecen de conocimientos digitales pueden no ser conscientes de que los agresores pueden utilizar tecnologías para controlarlas. En este sentido:

> Las mujeres necesitan adquirir competencia digital para garantizar su seguridad, tanto en línea, como fuera de línea. El conocimiento de cómo proteger los datos personales y garantizar la privacidad en línea es importante para todos/as los/as usuarios/as de internet, pero es particularmente esencial para las mujeres y las niñas, que tienen más probabilidad de volverse blanco de delitos por internet y de violencia de género en línea.[72]

70. West, M., Kraut, R., & Chew, H. E. (2019). *I'd blush if I could: Closing gender divides in digital skills through education*. EQUALS & UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000367416
71. Ibid.
72. Ibid.

Otros/as investigadores/as feministas creen que la brecha de acceso y habilidades digitales que afecta a las mujeres tiene que ver con las dinámicas de poder y los desequilibrios culturales, ya que el acceso lo suministran el Estado y el aparato estatal, y por ende se controla mediante otros sitios de poder, ya sean grandes corporaciones e instituciones como la escuela o la universidad, o la familia,[73] que son todos espacios donde suele perpetuarse la perspectiva hegemónica de las tecnologías.[74]

Factores demográficos en el comportamiento relativo a la ciberseguridad

La inclusión de interacciones humanas en la ciberseguridad ha llevado a varios/as investigadores/as del área de la "seguridad del comportamiento informático" a enfocarse en el estudio del nivel humano y su vulnerabilidad frente a los ciberataques, lo que puede producirse por negligencia, errores, enfermedad, muerte, amenazas por parte de personas enteradas y susceptibilidad a la ingeniería social.[75] En otras palabras, las medidas de seguridad para contrarrestar los ataques deben tener en cuenta aspectos socioculturales, más allá de controles técnicos,[76] ya que comprender las diferencias individuales en las conductas de ciberseguridad ayuda a la comunidad de investigación, a las organizaciones y a los/as empleados/as que trabajan en el sector de la seguridad a comprender y abarcar la sensibilidad ante ataques potenciales contra la seguridad.[77]

En este contexto, el análisis de aspectos demográficos de los individuos tales como la edad, el género, o el contexto educativo, apunta a brindar pistas sobre comportamientos de seguridad, aunque no siempre se analicen desde el contexto de las relaciones de poder y las jerarquías sociales, como en la teoría interseccional. Así, buena parte de esta investigación muestra evidencias sobre diferencias de género en cuanto a las creencias de ciberseguridad y las intenciones de comportamiento, además de basarse en factores psicológicos para explicar comportamientos relativos a la ciberseguridad.[78] Por tanto, los resultados varían: algunos estudios muestran que la eficacia de las mujeres en cuanto a la ciberseguridad es menor que la de los hombres; otros indican que el grado de conciencia de las mujeres en cuanto a la protección de sus datos personales es menor que el de los hombres; algunos señalan que la conducta de las mujeres en relación a la actualización de programas de software es

73. van der Spuy, A., & Aavriti, N. (2018). *Mapping research in gender and digital technology*. APC. https://www.apc.org/en/pubs/mapping-research-gender-and-digital-technology
74. Zanolli, B., Jancz, C., Gonzalez, C., Araujo dos Santos, D., & Prado, D. (2018). Feminist infrastructure and community networks: An opportunity to rethink our connections from the bottom up, seeking diversity and autonomy. In A. Finlay (Ed.), *Global Information Society Watch 2018: Community Networks*. IDRC & APC. https://giswatch.org/sites/default/files/gw2018_t7_feminist_infrastrucutre.pdf
75. Cuchta, T., Blackwood, B., Devine, T. R., Niichel, R. J., Daniels, K. M., Lutjens, C. H., Maibach, S., & Stephenson, R. J. (2019). Human Risk Factors in Cybersecurity. *SIGITE '19: Proceedings of the 20th Annual SIG Conference on Information Technology Education*. https://doi.org/10.1145/3349266.3351407
76. Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures, computers & security. *Computers & Security, 97*. https://doi.org/10.1016/j.cose.2020.101931
77. Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358. https://doi.org/10.1016/j.cose.2017.11.015
78. Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443. https://doi.org/10.1016/j.chb.2016.12.040

mejor que la de los hombres; y otros parecen indicar que existe una relación entre la inestabilidad emocional de las mujeres y el hecho de ser más vulnerables a situaciones de phishing.[79] En este marco, el papel del género en los comportamientos relativos a la ciberseguridad aún no está claro y merece un análisis más profundo.[80] Sin embargo, habría que examinar con cuidado estos resultados, así como las metodologías utilizadas, especialmente cuando no dejan espacio para las contribuciones de la teoría interseccional de género, que podría ayudar a complejizar la mirada y a evitar caer en la biologización y la universalización de las diferencias culturales entre hombres y mujeres. Algunas voces críticas señalan, por ejemplo, que:

> La literatura sobre el comportamiento sexual y de seguridad está muy mezclada, de forma que algunos/as investigadores/as encontraron diferencias según el sexo, mientras que otros/as no. Nuestra posición es que cualquier diferencia hipotéticamente presente es una diferencia construida socialmente, no una causada genéticamente y, por ende, implica analizar las características atribuidas a los sexos como manifestación de una expresión idealizada de género, en lugar de analizar simplemente el sexo.[81]

79. Ergen, A., Ünal, A. N., & Saygili, M. S. (2021). Is It Possible to Change the Cyber Security Behaviours of Employees? Barriers and Promoters. *Academic Journal of Interdisciplinary Studies, 10*(4). https://doi.org/10.36941/ajis-2021-0111
80. McGill, T. J., & Thompson, N. (2018). Gender Differences in Information Security Perceptions and Behaviour. In *Australasian Conference on Information Systems 2018*. University of Technology Sydney ePress. https://dx.doi.org/10.5130/acis2018.co
81. Hull, M. (2015). *Factors affecting secure computer behaviour*. Tesis de maestría, Universidad de Carleton. https://curve.carleton.ca/system/files/etd/d2e61738-e6e1-4f3d-8e6e-aa1ba1bc7d38/etd_pdf/3c351dac4dd33a4bf5057bdcc66e1366/hull-factorsaffectingsecurecomputerbehaviour.pdf

D) IMPACTO DIFERENCIADO DE CIBERINCIDENTES SEGÚN EL GÉNERO

La gente experimenta las amenazas en línea de manera diferente según su identidad y su experiencia, de modo que es necesario entender que hay que tener en cuenta la cuestión de género en lo que se considera una "amenaza" para la ciberseguridad. En otras palabras, las amenazas "tradicionales" de la ciberseguridad, tales como el espionaje, el robo económico, la intromisión, o la alteración de dispositivos personales y redes tienen diferentes consecuencias según el género de los individuos afectados, entre otros factores interseccionales.[82] Del mismo modo, se reconoce que los ataques catalogados como violencia de género en internet, tales como el doxeo, el ciberacoso y la difusión no consensuada de imágenes íntimas, también pueden darse a partir de la intromisión, o la alteración de las redes y los dispositivos personales.[83]

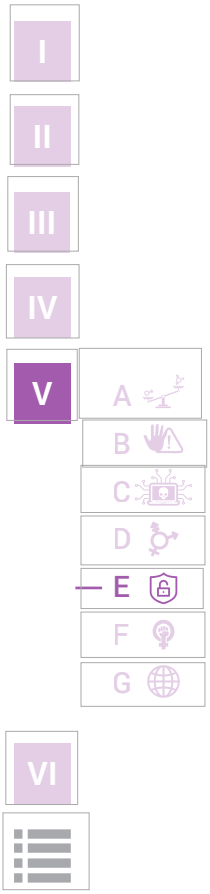
Un caso clásico de análisis consiste en los diversos grados en que se ven afectadas las personas por la fuga de datos. Es decir, suponiendo que la recolección de datos nunca ocurre en un ambiente neutro en términos de género, cuando se filtran datos, es probable que el impacto sea más severo entre las mujeres y las personas LGBTQI+ a causa de las desigualdades históricas y estructurales que existen en las relaciones de poder, con base en el género y la sexualidad.[84] Otro fenómeno analizado ampliamente son los intentos del Estado de gestionar y gobernar las redes, a raíz de lo cual los apagones cada vez más frecuentes de internet crean vulnerabilidades particulares para las mujeres y las comunidades marginadas. Así, hay registro de que los apagones de internet tienen un efecto particularmente adverso entre las mujeres que, en sus realidades locales, no pueden tener una presencia en los espacios públicos tradicionales, por lo cual no tienen acceso a internet y consecuentemente, carecen de acceso a la información, lo que resulta en detrimento de sus derechos y libertades.[85] En Uganda, por ejemplo, los

82. Brown, D., & Pytlak, A. (2020). Op. cit.; Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.
83. Millar, K., Shires, J., & Tropina, T. Op. cit.
84. Brown, D., & Pytlak, A. (2020). Op. cit.
85. Johri, N. (2020, 13 November). India's internet shutdowns function like 'invisibility cloaks'. *DW*. https://www.dw.com/en/indias-internet-shutdowns-function-like-invisibility-cloaks/a-55572554

apagones de internet afectaron su rol esencial en el desarrollo nacional ya que son las mujeres urbanas las que acceden regularmente a programas de desarrollo en línea.[86] Brown y Pytlak identifican las consecuencias de los apagones de internet en la seguridad personal de las mujeres y las personas LGBTQI+ que utilizan sus dispositivos móviles y canales de comunicación como herramienta de seguridad, así como en los costos económicos y profesionales que pagan las mujeres en la economía formal e informal, los efectos sobre el bienestar emocional y, por supuesto, a nivel educativo, cuando las mujeres son relegadas de los espacios tradicionales e internet constituye una oportunidad de acceso a la educación.[87]

86. Aceng, S. (2020, 15 December). Internet Shutdowns: An Evaluation of Women's Online Expression and Participation in Uganda. *The GNI Blog*. https://medium.com/global-network-initiative-collection/internet-shutdowns-an-evaluation-of-womens-online-expression-and-participation-in-uganda-8a4cac7bc479
87. Brown, D., & Pytlak, A. (2020). Op. cit.

E) RECONFIGURAR LOS MARCOS DE ANÁLISIS DE LA CIBERSEGURIDAD



Los análisis de ciberseguridad suelen empezar con una "modelización de la amenaza": un análisis sistemático del perfil del posible atacante, los vectores de ataque más probables y los valores o bienes más deseados por un atacante. Así es como se supone, según Slupska, que la modelización de una amenaza refleja presupuestos sobre las causas de la inseguridad de los/as usuarios/as de tecnología.[88] Pero, como se mostró, las personas tienen diferentes experiencias de amenazas en línea según su identidad y su experiencia de vida. Por eso, muchos estudios están avanzando hacia la creación de nuevos marcos de ciberseguridad (utilizando los pilares básicos de diseño, defensa y respuesta prevalente entre practicantes y responsables de la formulación de políticas), y dando pasos hacia la inclusión de consideraciones de género dentro de esos elementos.[89] De esta forma, la investigación en ciberseguridad que, de aquí en adelante, se enfoque en los grupos marginados puede habilitar el desarrollo de sistemas de ciberseguridad diseñados para ser más resilientes frente al abanico de amenazas al que realmente están sujetos los humanos.[90]

Por un lado, hay un pilar de diseño que, como dicen Millar et al., se propone incorporar seguridad a los sistemas sociotecnológicos a fin de prevenir, o mitigar vulnerabilidades y ataques.[91] El concepto de ciberseguridad que se emplea en el diseño tecnológico tiene en cuenta al género ya que los modelos de amenaza, la notificación del/a usuario/a y los procedimientos de control, además de la publicidad de las tecnologías de ciberseguridad, implican una mayor probabilidad de reducir u omitir las amenazas de ciberseguridad contra las mujeres (o los grupos de género que se encuentran en una posición más vulnerable en un contexto determinado);[92] que haya más carga de seguridad agregada; y que sea más probable que las mujeres y otros grupos vulnerables se vean afectados por la publicidad sobre ciberseguridad que no es ingenua en relación a los peligros que corren.[93] Slupksa y Tanczer tienen presente que las estrategias de mitigación técnica no servirán para "resolver" por completo los problemas de abuso tecnológico en el contexto de la violencia de género perpetrada mediante el uso de IoT (internet of things o "internet de las cosas"). Por ello, creen que en lugar de tratar de eliminar toda fuente de vulnerabilidad, lo

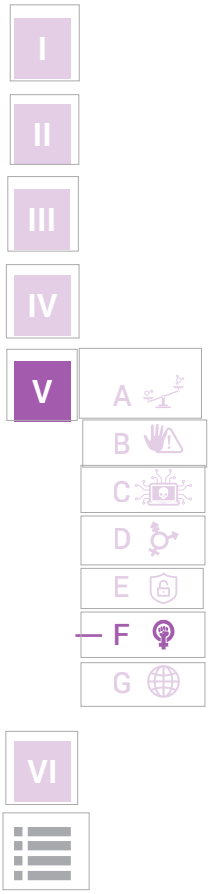
88. Slupska, J. (2019). Op. cit.
89. Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.
90. Slupska, J., Dawson Duckworth, S., Ma, L., & Neff, G. (2021). Op. cit.
91. Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.
92. Slupska, J., Dawson Duckworth, S., Ma, L., & Neff, G. (2021). Op. cit.
93. Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.

más ventajoso para los actores industriales sería pensar en modelos de diseño convenientes que, por ejemplo, mejoren la usabilidad del diseño para las personas que sufren abusos y hagan las cosas más difíciles para quienes perpetran los abusos.[94] Además, el sector de la tecnología debería ser lo suficientemente flexible como para modificar y rediseñar sistemas después de su implementación, lo que sería beneficioso para las víctimas/sobrevivientes de violencia de género y para la comunidad de usuarios/as en general debido a las mejoras de seguridad y privacidad que se pueden diseñar e implementar. También hay consenso sobre la necesidad de que el pilar del diseño sea participativo, por ejemplo, desarrollar metodologías para escuchar las inquietudes de usuarios y usuarias en relación al alcance y la amplitud de los modelos de amenaza a la ciberseguridad. Para Slupska, Dawson Duckworth, Neff et al., se trata de crear modelos de amenazas para humanos, en lugar de hacerlo para sistemas.[95]

Millar et al. explican cómo influye el género sobre los pilares de las respuestas de defensa e incidente.[96] La defensa tiene normas muy asociadas a la masculinidad debido a sus raíces militares, de modo que se prioriza la idea de ciberseguridad para los Estados y las corporaciones, dejando atrás a las personas. Las normas de género en relación a la vulnerabilidad pueden hacer que se vuelva difícil aceptar los errores, buscar ayuda, o trabajar en colaboración, generando una resistencia a implementar defensas de ciberseguridad en forma eficiente y a mejorar la transparencia en cuanto a la información sobre incidentes de ciberseguridad. En el momento de dar respuesta a un incidente, hay varios aspectos a considerar desde el punto de vista del género: la prioridad que se le da a los ataques corporativos por sobre los que afectan a los individuos, la manera en que se presta ayuda utilizando un lenguaje altamente codificado, la revictimización de las víctimas (por ejemplo, acusándolas por los ataques recibidos), o la composición excesivamente masculinizada de los Equipos de Respuesta ante Emergencias Informáticas (CERT, por su sigla en inglés).

94. Slupksa, J., & Tanczer, L. (2021). Op. cit.
95. Slupska, J., Dawson Duckworth, S., Neff, G., et al. (2021). Op. cit.
96. Millar, K., Shires, J., & Tropina, T. (2021). Op. cit.

F) INFRAESTRUCTURA DE UNA INTERNET AUTÓNOMA Y FEMINISTA

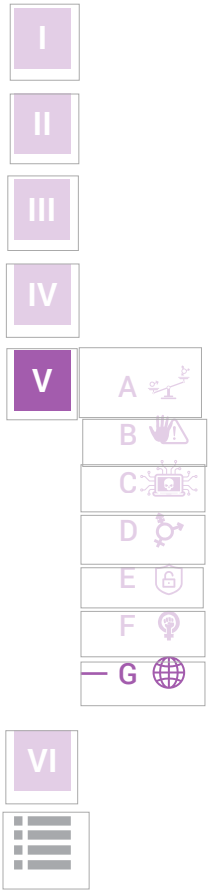


La infraestructura actual de internet está diseñada y pensada de una forma que casi no tiene en cuenta las experiencias localizadas. Eso también explica por qué las plataformas comerciales perpetúan formas de violencia contra las mujeres de larga data, ofreciendo escasos instrumentos para lidiar con esas situaciones en forma adecuada. En otras palabras, la mayor parte de las relaciones y las elecciones tecnopolíticas que hay detrás de estos dispositivos no responden a las necesidades de los grupos que se ven afectados por desigualdades estructurales tales como el género, la raza, la etnicidad y la clase social.[97] Para dar respuesta a esta realidad, el feminismo se ocupa de la infraestructura de internet, con el fin de terminar con las universalizaciones y aliviar experiencias locales y específicas mediante asociaciones e intercambio de conocimiento y técnicas.[98] El diseño y desarrollo de infraestructuras autónomas se propone crear independencia y sistemas económicos alternativos, intercambio, crecimiento, trabajo y cuidado y respeto mutuos.[99] Prado et al. señalan incluso que agregarle la palabra "feminista" a las infraestructuras y proponer la perspectiva interseccional, o las solidaridades sociales ayuda a destacar la no neutralidad de las tecnologías y los dispositivos que sirven al funcionamiento de internet.[100] También proponen un cambio de abordaje en la ciberseguridad: dejar el concepto centrado en la importancia de la privacidad individual y la necesidad de protegerse y defenderse de ataques, para pasar a una concepción colectiva de cuidado y ética dentro y fuera de las comunidades. En particular, muestran la necesidad de construir espacios en línea y fuera de línea libres de ataques, donde se garantice libertad de expresión a las mujeres, las poblaciones negras y las personas LGBTQI, entre otras.[101]

Una parte fundamental de esta infraestructura feminista es el desarrollo de redes comunitarias. Junto con la infraestructura feminista, estas redes comunitarias constituyen un desafío al androcentrismo y el colonialismo, y critican la idea hegemónica de que estas redes sólo han sido concebidas para el acceso sin tener en cuenta los protocolos, ni el diseño de software e infraestructura, además de otras acciones colectivas para el bienestar de las mujeres en su diversidad.[102]

97. Prado, D., de Araújo, D. C., & Mourão Kanashiro, M. (2020). Tecnologias, infraestruturas e redes feministas: potências no processo de ruptura com o legado colonial e androcêntrico. *Cadernos Pagu, 59*. https://doi.org/10.1590/18094449202000590003; Lobato, L. C., & Gonzalez, C. (2020). Embodying the web, recoding gender: How feminists are shaping progressive politics in Latin America. *First Monday, 25*(5). https://doi.org/10.5210/fm.v25i5.10129
98. Prado, D., de Araújo, D. C., & Mourão Kanashiro, M. (2020). Op. cit.
99. van der Spuy, A., & Aavriti, N. (2018). Op. cit.
100. Prado, D., de Araújo, D. C., & Mourão Kanashiro, M. (2020). Op. cit.
101. van der Spuy, A., & Aavriti, N. (2018). Op. cit.; Zanolli, B., Jancz, C., Gonzalez, C., dos Santos, D. A., & Prado, D. (2018). Op. cit.
102. Zanolli, B., Jancz, C., Gonzalez, C., dos Santos, D. A., & Prado, D. (2018). Op. cit.

G) POLÍTICAS PÚBLICS INTERNACIONALES DE CIBERSEGURIDAD



Vale la pena destacar el ímpetu que agendas tales como la de Mujeres, paz y seguridad le han dado al abordaje de género en la política pública internacional de ciberseguridad.

Ya hace algún tiempo que los/as investigadores/as feministas sobre relaciones internacionales cuestionan los estudios de seguridad convencionales debido a conceptos binarios de violencia interna/externa y personal/política, así como la visión de los conflictos desde una perspectiva vertical, o estructural. La comunidad de investigación feminista, en cambio, adoptó un abordaje desde las bases para analizar el impacto de la guerra a nivel micro.[103] En con-sonancia con esto, la Agenda Mujeres, Paz y Seguridad logró el consenso en cuanto a que las mujeres se ven mucho más afectadas por los conflictos y otras amenazas contra la paz y la seguridad internacional.[104]

A pesar de todos estos avances, muchas veces se mantiene la separación entre los derechos humanos y la "seguridad internacional". Así, aunque los derechos humanos deberían tenerse en cuenta en el diálogo acerca de la ciberseguridad internacional, la realidad es que rara vez sucede. El resultado es que se sabe poco sobre la manera en que las ciberoperaciones internacionales maliciosas que se realizan entre Estados afectan a las personas según su género, o según otras características que pueden volverlas vulnerables.[105] Más aún, a pesar de la evidencia de que la desigualdad y la discriminación que subyace al género y otras características interseccionales también influyen sobre el tipo de consecuencias experimentadas en un incidente ocurrido en el ciberespacio, el abordaje de Mujeres, paz y seguridad no se ha aplicado sistemáticamente al ciberespacio. Por ello hay escasez de datos para entender y enfrentar mejor a nivel de la seguridad internacional la diferencia de impacto en el dominio de las TIC.[106]

103. Tickner, J. A. (2004). Op. cit.
104. Naciones Unidas. (2002). *Women, Peace and Security*. Study submitted by the Secretary-General pursuant to Security Council resolution 1325 (2000). https://www.un.org/womenwatch/daw/public/eWPS.pdf
105. Slupska, J. (2019). Op. cit.; Brown, D., & Pytlak, A. (2020). Op. cit.
106. Brown D., & Pytlak, A. (2020). Op. cit.; Sharland, L., et al. (2021). Op. cit.

De todas maneras, en los últimos tiempos los procesos multilaterales sobre ciberseguridad empezaron a incluir declaraciones oficiales que llaman la atención hacia la dimensión de género, pero aún de manera muy tímida y limitada, como sucede con el informe final del Grupo de trabajo de composición abierta de Naciones Unidas sobre ciberseguridad. Sin duda, a pesar de que numerosas delegaciones han establecido la necesidad de incluir la dimensión de género a la hora de implementar las normas cibernéticas, así como la necesidad de fomentar y enseñar la conciencia de género, y entender mejor los vínculos existentes entre las diversas concepciones sobre ciberseguridad y sobre la igualdad de género, no se ha registrado un gran avance.[107]

107. Ferrari, V. (2021). Why should gender matter (more) for the OEWG? *Cyber Peace & Security Monitor, 1*(10). https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.10.pdf

VI. CONCLUSIONES

Este análisis de la literatura sobre ciberseguridad y género reúne información de diversas fuentes que operan desde perspectivas diferentes en relación al género en el área de la ciberseguridad. Estos diversos abordajes analizan la cuestión de género en el contexto de relaciones de poder desiguales y también como mero factor demográfico. Sin embargo, a pesar de la gran diversidad, se puede apreciar que hay conceptos transversales de coincidencia y temas específicos para los cuales se reúnen más estudios y más evidencia. Mostramos que cada vez existe más interés en este tema aunque aún no haya un cuerpo más o menos ordenado de teoría y práctica. En este sentido, este documento propone un orden que puede ayudar a las organizaciones, la academia y los y las responsables de formular políticas a proponer sus propios mapas de progreso para profundizar en el conocimiento y/o aumentar el alcance del conocimiento en otras áreas de la ciberseguridad que aún no hayan sido estudiadas desde una perspectiva de género.

BIBLIOGRAFÍA

Para realizar este análisis sobre las publicaciones en el área del género y la ciberseguridad, se consultaron las siguientes fuentes:

Aceng, S. (2020, 15 December). Internet Shutdowns: An Evaluation of Women's Online Expression and Participation in Uganda. *The GNI Blog*. https://medium.com/global-network-initiative-collection/internet-shutdowns-an-evaluation-of-womens-online-expression-and-participation-in-uganda-8a4cac7bc479

Álvarez, D., & Vera, F. (2017). Ciberseguridad y derechos humanos en América Latina. In A. del Campo (Ed.), *Hacia una internet libre de censura II: Perspectivas en América Latina*. Universidad de Palermo. https://www.palermo.edu/cele/pdf/investigaciones/Hacia_una_internet_libre_de_censura_II.pdf

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437-443. https://doi.org/10.1016/j.chb.2016.12.040

Bardzell, S. (2010). Feminist HCI: Taking stock and outlining an agenda for design. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*. https://doi.org/10.1145/1753326.1753521

Barrett, F. J. (1996). The Organizational Construction of Hegemonic Masculinity: The Case of the US Navy. *Gender, Work & Organisation, 3*(3), 129-142. https://doi.org/10.1111/j.1468-0432.1996.tb00054.x

Barsh, J., & Yee, L. (2011). *Unlocking the full potential of women in the US economy*. McKinsey & Company.

Blair, J. R. S., Hall, A. O., & Sobiesk, E. (2019). Educating Future Multidisciplinary Cybersecurity Teams. *Computer, 52*(3), 58-6. https://doi.org/10.1109/MC.2018.2884190

Burrell, D. (2018). An exploration of the cybersecurity workforce shortage. *International Journal of Hyperconnectivity and the Internet of Things*, 2(1). http://dx.doi.org/10.4018/IJHIoT.2018010103

Brown, D., & Esterhuysen, A. (2019, 28 November). Why cybersecurity is a human rights issue, and it is time to start treating it like one. *APC*. https://www.apc.org/en/node/35879

Brown, D., & Pytlak, A. (2020). *Why Gender Matters in International Cyber Security*. Women's International League for Peace and Freedom and the Association for Progressive Communications. https://www.apc.org/en/pubs/why-gender-matters-international-cyber-security

Chowdhury, N. H., Adam, M. T. P., & Teubner, T. (2020). Time pressure in human cybersecurity behavior: Theoretical framework and countermeasures, computers & security. *Computers & Security, 97*. https://doi.org/10.1016/j.cose.2020.101931

Collins, P. (2019). *Intersectionality as Critical Social Theory*. Duke University Press.

Cuchta, T., Blackwood, B., Devine, T. R., Niichel, R. J., Daniels, K. M., Lutjens, C. H., Maibach, S., & Stephenson, R. J. (2019). Human Risk Factors in Cybersecurity. SIGITE '19: *Proceedings of the 20th Annual SIG Conference on Information Technology Education*. https://doi.org/10.1145/3349266.3351407

Deibert, R. (2018). Toward a Human-Centric Approach to Cybersecurity. *Ethics & International Affairs, 32*(4), 411-424. https://doi.org/10.1017/S0892679418000618

Deibert, R. (2018). Trajectories for future cybersecurity research. In A. Gheciu & W. C. Wohlforth (Eds.), *The Oxford Handbook of International Security*.

D'Hondt, K. (2016). *Women and Cybersecurity*. Master's thesis, Harvard Kennedy School.

Di Meco, L. (2019). *#SHEPERSISTED: Women, Politics & Power in the New Media World*. https://www.iknowpolitics.org/sites/default/files/191105shepersisted_final.pdf

Di Meco, L. (2020). *Online Threats to Women's Political Participation and The Need for a Multi-Stakeholder, Cohesive Approach to Address Them*. UN Women. EGM/CSW/2021/EP8. https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/CSW/65/EGM/Di%20Meco_Online%20Threats_EP8_EGMCSW65.pdf

Dunn Cavelty, M. (2018). Cybersecurity Research Meets Science and Technology Studies. *Politics and Governance*, 6(2), 22-30. https://www.cogitatiopress.com/politicsandgovernance/article/download/1385/1385

Ergen, A., Ünal, A. N., & Saygili, M. S. (2021). Is It Possible to Change the Cyber Security Behaviours of Employees? Barriers and Promoters. *Academic Journal of Interdisciplinary Studies, 10*(4). https://doi.org/10.36941/ajis-2021-0111

EU Disinfo Lab. (2021, 24 May). Why Disinformation is a Cybersecurity Threat. https://www.disinfo.eu/advocacy/why-disinformation-is-a-cybersecurity-threat

Ferrari, V. (2021). Why should gender matter (more) for the OEWG? *Cyber Peace & Security Monitor, 1*(10). https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.10.pdf

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345-358. https://doi.org/10.1016/j.cose.2017.11.015

Haciyakupoglu, G., & Wong, Y. (2021). *Gender, Security and Digital Space: Issues, Policies, and the Way Forward*. S. Rajaratnam School of International Studies. https://www.rsis.edu.sg/rsis-publication/cens/gender-security-and-digital-space-issues-policies-and-the-way-forward

Harris, B. A., & Woodlock, D. (2019). Digital Coercive Control: Insights from two landmark domestic violence studies. *The British Journal of Criminology, 59*(3), 530-550. https://doi.org/10.1093/bjc/azy052

Hull, M. (2015). *Factors affecting secure computer behaviour*. Tesis de maestría, Universidad de Carleton. https://curve.carleton.ca/system/files/etd/d2e61738-e6e1-4f3d-8e6e-aa1ba1bc7d38/etd_pdf/3c351dac4d-d33a4bf5057bdcc66e1366/hull-factorsaffectingsecurecomputerbehaviour.pdf

International Telecommunication Union. (2021). *Measuring digital development: Facts and figures 2021*. https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx

(ISC)². (2021). *In Their Own Words: Women and People of Color Detail Experiences Working in Cybersecurity*. https://www.isc2.org/-/media/ISC2/DEI/DEI-Market-Research-2021.ashx

Johri, N. (2020, 13 de noviembre). India's internet shutdowns function like 'invisibility cloaks'. *DW*. https://www.dw.com/en/indias-internet-shutdowns-function-like-invisibility-cloaks/a-55572554

Judson, E., Atay, A., Krasodomski-Jones, A., & Smith, J. (2020). *Engendering hate: The contours of state-aligned gendered disinformation online*. Demos. https://apo.org.au/sites/default/files/resource-files/2020-10/apo-nid309184.pdf

Kazansky, B. (2021). 'It depends on your threat model': the anticipatory dimensions of resistance to data-driven surveillance. *Big Data & Society, 8*(1). https://doi.org/10.1177/2053951720985557

King-Close, A. M. (2016). *A gender analysis of cyber war*. Tesis de maestría, Harvard Extension School.

Kumar, S. (2021). The missing piece in human-centric approaches to cybernorms implementation: The role of civil society. *Journal of Cyber Policy, 6*(3), 375-393. https://doi.org/10.1080/23738871.2021.1909090

Leitao, R. (2019). Anticipating Smart Home Security and Privacy Threats with Survivors of Intimate Partner Abuse. *DIS '19: Proceedings of the 2019 on Designing Interactive Systems Conference*. https://doi.org/10.1145/3322276.3322366

Lobato, L. C., & Gonzalez, C. (2020). Embodying the web, recoding gender: How feminists are shaping progressive politics in Latin America. *First Monday, 25*(5). https://doi.org/10.5210/fm.v25i5.10129
McGill, T. J., & Thompson, N. (2018). Gender Differences in Information Security Perceptions and Behaviour. *In Australasian Conference on Information Systems 2018*. University of Technology Sydney ePress. https://dx.doi.org/10.5130/acis2018.co

Millar, K., Shires, J., & Tropina, T. (2021). *Gender approaches to cybersecurity: Design, defence and response*. United Nations Institute for Disarmament Research. https://doi.org/10.37559/GEN/21/01

Myrttinen, H. (2020). *Tool 1: Security Sector Governance, Security Sector Reform and Gender*. DCAF, OSCE/ODIHR & UN Women. https://www.dcaf.ch/tool-1-security-sector-governance-security-sector-reform-and-gender

Nieminen, L. (2021). *Why is human trafficking excluded from the EU's cybersecurity?: An explorative study about cybersecurity and human trafficking in the European Union*. http://urn.kb.se/resolve?urn=urn:nbn:se:fhs:diva-9698

Nissenbaum, H. (2005). Where computer security meets national security. E*thics and Information Technology, 7*, 61-73. https://doi.org/10.1007/s10676-005-4582-3

Parkin, S., Patel, T., Lopez-Neira, I., & Tanczer, L. (2019). Usability analysis of shared device ecosystem security: Informing support for survivors of IoT-facilitated tech-abuse. *Proceedings of the New Security Paradigms Workshop (NSPW '19)*. https://doi.org/10.1145/3368860.3368861

Pierce, J., Fox, S., Merrill, N., & Wong, R. (2018). Differential Vulnerabilities and a Diversity of Tactics: What Toolkits Teach Us about Cybersecurity. *Proceedings of the ACM on Human-Computer Interaction, 2*. https://doi.org/10.1145/3274408

Poster, W. R. (2018, 26 March). Cybersecurity needs women. *Nature*. https://www.nature.com/articles/d41586-018-03327-w

Prado, D., de Araújo, D. C., & Mourão Kanashiro, M. (2020). Tecnologias, infraestruturas e redes feministas: potências no processo de ruptura com o legado colonial e androcêntrico. *Cadernos Pagu, 59*. https://doi.org/10.1590/18094449202000590003

Pytlak, A. (2021). Bringing gender analysis into international cybersecurity. *Cyber Peace & Security Monitor, 1*(8). https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.8.pdf

Reid, R., & Van Niekerk, J. (2014). From information security to cyber security cultures. *Information Security for South Africa 2014*. https://ieeexplore.ieee.org/document/6950492

Sharland, L., et al. (2021). *System Update: Towards a Women, Peace and Cybersecurity Agenda*. UNIDIR. https://doi.org/10.37559/GEN/2021/03

Shoker, S. (2021). *Making gender visible in digital ICTs and international security*. Report submitted to Global Affairs Canada. https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/oewg/documents/research-canada-1.pdf

Šimonović, D. (2018). *Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos*. A/HRC/38/47. https://undocs.org/A/HRC/38/47

Šimonović, D. (2018). *Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias sobre la violencia contra la mujer en la política*. A/73/301. https://undocs.org/A/73/301

Slupska, J. (2019). Safe at Home: Towards a feminist critique of cybersecurity. *St. Anthony's International Review, 15*. https://ssrn.com/abstract=3429851

Slupska, J., Dawson Duckworth. S., Ma, L., & Neff, G. (2021). Participatory threat modelling: Exploring paths to reconfigure cybersecurity. *Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems*. https://doi.org/10.1145/3411763.3451731

Slupska, J., Dawson Duckworth, S., Neff, G., et al. (2021). *Reconfigure: Feminist Action Research in Cybersecurity*. Reconfigure Network. https://www.oii.ox.ac.uk/news-events/news/reconfigure-feminist-action-research-in-cybersecurity

Slupska, J., & Tanczer, L. M. (2021). Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things. In J. Bailey, A. Flynn & N. Henry (Eds.), *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited. https://doi.org/10.1108/978-1-83982-848-520211049

Tickner, J. A. (2004). Feminist responses to international security studies. *Peace Review, 16*(1), 43-48. https://doi.org/10.1080/1040265042000210148

UNIDIR. (2021). *Fact sheet: Gender in cyber diplomacy*. https://unidir.org/publication/fact-sheet-gender-cyber-diplomacy

United Nations. (2002). *Women, Peace and Security*. Study submitted by the Secretary-General pursuant to Security Council resolution 1325 (2000). https://www.un.org/womenwatch/daw/public/eWPS.pdf

van der Spuy, A., & Aavriti, N. (2018). *Mapping research in gender and digital technology*. APC. https://www.apc.org/en/pubs/mapping-research-gender-and-digital-technology

Wajcman, J. (2000). Reflections on Gender and Technology Studies: In What State is the Art? *Social Studies of Science, 30*(3), 447-464. https://doi.org/10.1177/030631200030003005

West, M., Kraut, R., & Chew, H. E. (2019). *I'd blush if I could: Closing gender divides in digital skills through education*. EQUALS & UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000367416

Zanolli, B., Jancz, C., Gonzalez, C., Araujo dos Santos, D., & Prado, D. (2018). Feminist infrastructure and community networks: An opportunity to rethink our connections from the bottom up, seeking diversity and autonomy. In A. Finlay (Ed.), *Global Information Society Watch 2018: Community Networks*. IDRC & APC. https://giswatch.org/sites/default/files/gw2018_t7_feminist_infrastrucutre.pdf

Zimmermann, V., & Renaud, K. (2019). Moving from a "human-as-problem" to a "human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, 169-187. https://doi.org/10.1016/j.ijhcs.2019.05.005

APC
ASOCIACIÓN PARA
EL PROGRESO DE
LAS COMUNICACIONES