Enfoques de género en la ciberseguridad:
diseño, defensa y respuesta

KATHARINE MILLAR | JAMES SHIRES | TATIANA TROPINA

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

www.unidir.org

Enfoques de género en la ciberseguridad: diseño, defensa y respuesta

Agradecimientos

El apoyo de los patrocinadores principales de UNIDIR provee la base para todas las actividades del Instituto. Este proyecto de investigación recibió el apoyo de los gobiernos de Alemania, España, Irlanda, Noruega, Reino Unido, Suecia y Suiza.

Este informe se publicó originalmente en inglés en febrero de 2021. UNIDIR desea expresar su agradecimiento al Programa de Ciberseguridad del Comité Interamericano contra el Terrorismo de la Organización de los Estados Americanos (OEA) por traducir esta investigación y ponerla a disposición en español.

Las autoras y el autor desean agradecer a las siguientes personas y organizaciones por su generosa retroalimentación, tiempo y experticia aportados a esta investigación y la revisión de este informe.

- **Marwa Azelmat,** Association for Progressive Communications
- **Winnona DeSombre**, Google
- **Avri Doria,** Technicalities
- **Eugenia Dorokhova,** Geneva Centre for Security Sector Governance
- **Serge Droz,** Forum of Incident Response and Security Teams
- **Verónica Ferrari,** Association for Progressive Communications
- **Lenka Filipová,** United Nations Institute for Disarmament Research
- **Noelia Garcia Nebra,** International Organization for Standardization
- **Joyce Hakmeh,** Chatham House
- **Renata Hessmann Dalaqua,** United Nations Institute for Disarmament Research
- **Louise Marie Hurel Silva Dias,** Department of Media and Communications, London School of Economics
- **Aiko Holvikivi,** London School of Economics Centre for Women, Peace and Security
- **Jaana Holvikivi,** Helsinki Metropolia University of Applied Sciences
- **Edward Humphreys,** Convenor of the ISO/CEI Joint Technical Committee SC 27/WG 1
- **Andraz Kastelic,** United Nations Institute for Disarmament Research
- **Franziska Klopfer,** Geneva Centre for Security Sector Governance
- **Catalin Marinescu,** International Telecommunication Union
- **Beatrice Martini,** Access Now Digital Security Helpline

- **Niels ten Oever,** University of Amsterdam
- **Christine Runeggar,** Internet Society
- **Toby Shulruff,** National Network to End Domestic Violence
- **Julia Slupska,** University of Oxford
- **Leonie Tanczer,** University College London
- **Tracy Tuplin,** International Telecommunication Union
- **Kerstin Vignard,** United Nations Institute for Disarmament Research
- **Julia Voo,** Harvard Kennedy School
- **Daniel Woods,** University of Vienna

Notas

Las designaciones empleadas y la presentación del material en esta publicación no implican la expresión de ninguna opinión de ningún tipo por parte de la Secretaría de las Naciones Unidas con respecto a la condición jurídica de ningún país o territorio, ninguna ciudad o área, ni de sus autoridades o con relación a la delimitación de sus fronteras o límites. Los puntos de vista expresados en esta publicación son responsabilidad exclusiva de sus autoras/es. No reflejan necesariamente los puntos de vista ni las opiniones de las Naciones Unidas, UNIDIR, los miembros de su personal o sus patrocinadores.

Para citar esta obra

K. Millar, J. Shires, and T. Tropina. 2021. *Enfoques de Género en la Ciberseguridad: Diseño, Defensa y Respuesta.* Instituto de las Naciones Unidas de Investigación sobre el Desarme: Ginebra.

Sobre UNIDIR

UNIDIR es un instituto autónomo del Sistema de las Naciones Unidas financiado por voluntarios. Al ser uno de los pocos institutos sobre políticas en el mundo que se enfoca en el desarme, UNIDIR genera conocimiento y promueve el diálogo y la acción sobre el desarme y la seguridad. Con sede en Ginebra, UNIDIR ayuda a la comunidad internacional a desarrollar ideas prácticas e innovadoras necesarias para encontrar soluciones a problemas críticos de seguridad.

Sobre el Programa de Género y Desarme

El Programa Género y Desarme busca contribuir a las metas estratégicas de lograr la igualdad de género en los foros sobre desarme y aplicar de manera eficaz las perspectivas de género en los procesos de desarme. Utiliza investigación original, actividades de divulgación y herramientas para apoyar a las partes interesadas en el desarme a traducir la concienciación sobre las cuestiones de género en acciones prácticas.

Sobre las personas autoras

La **Dra. Katharine Millar** es Profesora Adjunta de Relaciones Internacionales en el London School of Economics and Political Science (LSE) y tiene un doctorado de la Universidad de Oxford del Reino Unido. Sus intereses de investigación abarcan la relación entre género, sexualidad, política y violencia. Su investigación actual examina el género y la ciberseguridad, el género, la raza, el militarismo y el populismo contemporáneo y los componentes transnacionales de las muertes asociadas a la COVID 19. La Dra. Millar es miembro del Consejo Directivo de la revista Millennium y del Centre for Women, Peace and Security del LSE. Ha participado en procesos de consultoría sobre la Agenda Mujeres, Paz y Seguridad de las Naciones Unidas para varios gobiernos nacionales y organizaciones internacionales, incluyendo el Reino Unido, Canadá y la Organización del Tratado del Atlántico Norte (OTAN).

El **Dr. James Shires** es Investigador Principal sobre ciberpolítica en Chatham House. Anteriormente, fuer Profesor Asistente en el Institute of Security and Global Affairs en la Universidad Leiden de los Países Bajos, y miembro de la Cyber Statecraft Initiative en el Atlantic Council. Tiene un Doctorado en Relaciones Internacionales de la Universidad de Oxford. Su investigación examina la gobernanza de la ciberseguridad, concentrándose en la interacción entre las amenazas a los individuos, los Estados y las organizaciones, las nuevas dinámicas de la política internacional y el desarrollo de experticia en ciberseguridad. Ha ganado premios del Hague Program on Cyber Norms, el German Marshall Fund y el International Institute for Strategic Studies (IISS).

La **Dra. Tatiana Tropina** es Profesora Adjunta de Gobernanza de la Ciberseguridad en el Institute of Security and Global Affairs en la Universidad Leiden y tiene un doctorado de Far Eastern Federal University de Rusia. Sus áreas de experticia incluyen las normas internacionales para la lucha contra el cibercrimen, investigaciones digitales y auto y coregulación para abordar temas de ciberseguridad y el enfoque multiparticipativo de la

ciberseguridad. Ha participado en proyectos de investigación legal, cibercrimen aplicado y ciberseguridad, tal como los estudios sobre el cibercrimen para el Simposio Mundial para Organismos Reguladores (2010) y la Oficina de las Naciones Unidas contra la Droga y el Delito (2012–2013), investigación sobre flujos financieros ilícitos y tecnologías digitales para el Informe sobre el Desarrollo Mundial 2016 y un proyecto con la Oficina de la Policía Criminal de Alemania Federal sobre cómo mejorar la asistencia legal mutua para interceptar comunicaciones electrónicas en la Unión Europea (2015–2018).

Tabla de contenido

Lista de abreviaturas

CEI	Comisión Electrotécnica Internacional
CERT	Equipo de Respuesta ante Emergencias Informáticas
GTCA	Grupo de Trabajo de Composición Abierta
IA	Inteligencia Artificial
IETF	Internet Engineering Task Force [Grupo de Trabajo en Ingeniería de Internet]
ISO	Organización Internacional de Normalización
TIC	Tecnologías de la Información y Comunicaciones
LBGTQ+	Lesbianas, gais, bisexuales y personas trans [transgénero, transexuales y travestis] y queer y personas de identidades y expresiones de género y orientaciones sexuales diversas
ODS	Objetivos de Desarrollo Sostenible
STEM	Ciencias, tecnología, matemáticas e ingeniería
TI	Tecnologías de la Información
UIT	Unión Internacional de Telecomunicaciones

Resumen ejecutivo

Los procesos multilaterales sobre ciberseguridad recientemente han empezado a incluir declaraciones oficiales que llaman la atención hacia sus dimensiones de género. Varias delegaciones que participan en el Grupo de Trabajo de Composición Abierta (GTCA) de las Naciones Unidas sobre los avances en el campo de la informatización y las telecomunicaciones en el contexto de la seguridad internacional han manifestado la necesidad de incorporar el género en la implementación de las normas sobre informática y en el desarrollo de capacidades sensibles en cuanto al género, además de entender mejor los vínculos entre la ciberseguridad y los marcos sobre la igualdad de género. Sin embargo, sigue habiendo preguntas sobre la aplicación general de las perspectivas de género a la ciberseguridad, así como también sobre cuáles tipos de acciones se necesitan para implementar eficazmente un enfoque de género a la ciberseguridad y volver estas metas en realidad.

Para enfrentar esta brecha de conocimiento, este informe delinea la relevancia de las normas de género para la ciberseguridad. Aprovecha la investigación existente, complementada con entrevistas con actores y personas expertas, para evaluar las diferencias basadas en género en los roles sociales y la interacción de mujeres, hombres y personas no binarias de todas las edades reflejadas en la distribución de poder (por ejemplo, la influencia sobre las decisiones políticas y la gobernanza corporativa), el acceso a recursos (tal como el acceso equitativo a educación, salarios y protección personal) y la construcción de normas y roles de género (como los supuestos sobre la víctimas y los responsables de la violencia facilitada por la informática).

En general, las normas de género informan la ciberseguridad de dos maneras. Primero, el género construye identidades individuales, roles y expectativas dentro de la ciberseguridad y en la sociedad en general, tal como la frecuente asociación de

experticia con los hombres y la masculinidad. Segundo, el género opera como una forma de estructura social jerárquica. Esto significa que las actividades y los conceptos asociados con la masculinidad, como la experticia técnica a menudo, pero no siempre, se valoran más que los asociados con las mujeres y la feminidad, tal como la experticia en comunicación o iniciativas de igualdad, diversidad e inclusión.

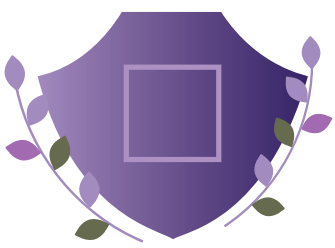
Para entender cómo el género da forma a actividades específicas de ciberseguridad, este informe propone un nuevo marco centrado en lo cibernético con base en tres pilares: diseño, defensa y respuesta, los cuales están alineados a las perspectivas prevalentes de las y los profesionales en ciberseguridad y creadores de políticas. En cada uno de estos tres pilares, la investigación identifica dimensiones distintas de actividades relacionadas con lo cibernético que deben considerarse desde una perspectiva de género.

Diseño

El diseño de la tecnología es sesgado en cuanto al género: malinterpreta, omite y consolida ciertos usos sesgados en cuanto al género, privilegia las prácticas que se conciben como masculinas sobre las femeninas y esencializa la feminidad en formas problemáticas. El diseño de la ciberseguridad hereda estos problemas. Los modelos de amenazas, los procedimientos de notificación y control de personas usuarias y la publicidad de las tecnologías de ciberseguridad implican que las mujeres tengan más probabilidad de restar importancia a las amenazas u omitirlas, más probabilidad de tener cargas adicionales de seguridad y más probabilidad de ser afectadas por el mercadeo engañoso sobre ciberseguridad.

Defensa

Las simulaciones y caracterizaciones de la defensa contra las amenazas a menudo involucran estereotipos de género. En el fondo, la manera en que pensamos sobre la defensa (o sea, lo que significa defender y las acciones de sentido



común que tomamos para defender) refleja una serie de normas asociadas con la masculinidad, tal como protección, competencias técnicas y autonomía. Las normas de género alrededor de la vulnerabilidad pueden hacer que admitir un error, buscar ayuda o trabajar en colaboración sea más difícil, lo cual genera renuencia a buscar activamente la defensa de la ciberseguridad o de ejercer la transparencia.

Respuesta

Las respuestas de la ciberseguridad implican dinámicas de género distintivas. Las prioridades, la composición, las prácticas y horas de trabajo esperadas y la cultura en el lugar de trabajo de los equipos de respuesta a incidentes requieren un análisis de género. Además, la informalidad de las comunidades de respuesta a la ciberseguridad – a menudo compuestas por redes de confianza cerradas formadas a través de años de interacción – significa que en ellas puede haber una menor participación de mujeres y grupos minoritarios, incluso cuando se ajustan a las proporciones generales de la industria. Las respuestas de la ciberseguridad también pueden implicar una dinámica de género de culpar a la víctima, en la cual se percibe a las organizaciones o los individuos con insuficiente defensa de ciberseguridad o medidas de protección de la identidad como "si estuvieran pidiendo ser hackeadas".

Las investigaciones que analizan los vínculos entre el género y la ciberseguridad son escasas, pero están aumentando. Por ende, en cada uno de estos pilares, el informe destaca áreas donde se deben realizar investigaciones adicionales. Este informe también propone recomendaciones para la incorporación de las consideraciones de género en todas las políticas y prácticas de ciberseguridad, incluyendo las siguientes:

- Las normas de ciberseguridad tienen un importante papel que jugar en el desarrollo del diseño de tecnologías sensibles al género. Los creadores de normas deben evaluar hasta qué grado la equidad de género es parte de las normas de ciberseguridad, incluida la participación significativa, el contenido de las normas y su lenguaje y los efectos directos e indirectos sobre el género. El primer paso hacia

esto es la recopilación de datos desagregados por género en todas las políticas y prácticas de ciberseguridad.

- Los esfuerzos para abordar la brecha de género en la ciberseguridad deben aprovechar los movimientos más generales para aumentar la participación de las mujeres en ciencia, tecnología, ingeniería y matemáticas (STEM). Asimismo, es importante elevar el perfil y valor de las destrezas en ciberseguridad y la experticia más allá de STEM (tal como, la experticia en comunicación, ética o gobernanza legal). Todos los actores involucrados en la ciberseguridad deben contrarrestar las percepciones nocivas en cuanto al género y los estereotipos y deben apoyar los cambios organizativos y culturales que valoran las actividades y capacidades diversas.

- Las medidas legales en ciberseguridad deben incorporar una perspectiva de género en el desarrollo, la implementación, el control y la evaluación de las leyes relevantes. Las medidas legales deben estar sustentadas en procesos legislativos abiertos y participativos que involucren a todos los actores, especialmente los grupos y las organizaciones de la sociedad civil que promueven los derechos de los individuos de identidades de género subrepresentadas y marginalizadas.

- Todas las organizaciones – tanto en el sector público como en el privado – deben ofrecer capacitaciones sobre "género y ciberseguridad" para profesionales y creadores de políticas. Esta capacitación debe incorporar un enfoque dual: (a) igualdad de género, diversidad e inclusión en el lugar de trabajo y (b) el desarrollo de una perspectiva de género sobre ciberseguridad como una destreza profesional. Esta capacitación proveerá una introducción práctica al género como un elemento de la política, asegurando así que la experticia sobre género sea un aspecto fundamental y respetado de la práctica profesional de políticas de ciberseguridad y su creación.

- Los Estados que participan en los procesos de ciberseguridad en la ONU podrían apoyar y financiar la elaboración de una caja de herramientas de capacitación en informática y género y solicitar a las organizaciones del sector público y a contratistas del sector privado que la use cuando sea posible. Los actores no estatales en la academia y, particularmente, la sociedad civil podrían aportar su experticia en la creación de tal caja de herramientas, mientras que los actores corporativos podrían implementar versiones modificadas y usar sus ventajas comerciales para

asegurarse que otros lo hagan también. Los Estados también podrían usar la caja de herramientas para fomentar la cooperación interestatal en ciberseguridad.

Tales medidas garantizarían que la ciberseguridad mejorará la seguridad de las personas de todas las identidades y expresiones de género, además de la paz y seguridad internacionales. La conclusión fundamental es que estos dos niveles de seguridad no puede estar separados.

1. Introducción

Las dinámicas y los supuestos sesgados en cuanto al género son prevalentes en el campo de la ciberseguridad. Las amenazas contra la ciberseguridad las experimentan de manera diferente mujeres y niñas, hombres y niños y personas de identidades de género no binario.[1] Las personas de diferentes géneros también participan de manera desigual en la formación y promulgación de políticas y prácticas de ciberseguridad.[2]

Sin embargo, fue hasta hace poco que los procesos multilaterales sobre ciberseguridad empezaron a incluir declaraciones oficiales que llaman la atención a las dimensiones de género de la gobernanza de la ciberseguridad.[4] Es de notar que varias delegaciones que participan en el GTCA sobre avances en el campo de las TIC de la ONU en el contexto de la seguridad internacional han señalado la necesidad de incorporar el género en la implementación de las normas informáticas y en el desarrollo de capacidades sensibles al género, así como también un mejor entendimiento de los vínculos entre los marcos de ciberseguridad e igualdad de género.[5]

Género

Género se refiere a los roles, comportamientos y atributos construidos social y culturalmente que se asocian con la masculinidad y la feminidad en un tiempo y lugar dados. Las normas de género cambian con el tiempo e informan las identidades de los individuos, las relaciones sociales y la distribución de recursos y poder en la sociedad. Aunque el género a menudo se entiende socialmente como la expresión de expectativas con respecto al comportamiento de hombres y mujeres, el género es no binario y diverso. Se refiere a las personas de todas las identidades y expresiones de género.[3]

A pesar de este avance, la investigación existente sobre género y ciberseguridad es escasa. Esto se debe parcialmente a la percepción errónea común de que los aspectos técnicos o tecnológicos de la ciberseguridad son neutros en cuanto al género, y, por lo tanto, ciegos al género, sin efectos diferentes sobre los individuos de identidades y expresiones de género y sexuales marginalizadas (y otros grupos minoritarios).[6] Presumiblemente también se debe en parte al cambio iterativo y constante en el campo, que motiva a los expertos a priorizar el abordaje de los riesgos nuevos en vez de evaluar las implicaciones de género de las prácticas de ciberseguridad.

Para atacar esta brecha de conocimiento, este informe explora los problemas de ciberseguridad desde una perspectiva de género. Específicamente, la investigación responde las preguntas siguientes:

- ¿Cuáles son las principales implicaciones en cuanto al género de las políticas y prácticas de ciberseguridad?
- ¿Cómo estas implicaciones se abordan en la investigación y políticas actuales?
- ¿Qué acciones adicionales abordarían las desigualdades de género y los daños diferenciados de la ciberseguridad?

El informe responde la primera pregunta de investigación presentando en el capítulo 2 un nuevo marco centrado en lo cibernético, alineado con las perspectivas prevalentes sobre ciberseguridad entre personas profesionales y creadoras de políticas. Este marco se usa para organizar y analizar las implicaciones en cuanto al género de los sistemas, los procesos y las prácticas de ciberseguridad en tres pilares: diseño, defensa y respuesta. Luego cada pilar se discute por separado en los capítulos 3–5, que delinean el contenido del pilar y las dinámicas de género generales a nivel sectorial que son parte de este.

Para responder la segunda pregunta de investigación, la discusión de cada pilar también contiene un análisis más detallado de un caso de estudio ilustrativo: las normas de ciberseguridad, el talento y la experticia y las medidas legales. Para ayudar a las personas creadoras de políticas y profesionales a identificar las implicaciones de género e

Igualdad de género

Igualdad de género es el principio de que "mujeres y hombres, niñas, niños [y las personas no binarias] tienen condiciones, tratamiento y oportunidades iguales para realizar su máximo potencial, derechos humanos y dignidad y para contribuir al desarrollo económico, social, cultural y político (y beneficiarse de ello)".[7]

igualdad de los componentes técnicos de la ciberseguridad, respondemos la tercera pregunta de investigación resaltando las áreas claves que requieren investigación adicional, proporcionando un marco para la estructuración y síntesis de este trabajo futuro y planteando recomendaciones concretas sobre políticas. Al hacerlo, esperamos mejorar la ciberseguridad internacional al reducir las consecuencias negativas de los supuestos, sesgos y omisiones relacionados con el género.

2. Ciberseguridad y género

Este informe define la ciberseguridad como la prevención y mitigación de la interferencia maliciosa mediante dispositivos y redes digitales. La interferencia maliciosa, a su vez, se define como la intrusión ilegítima o interrupción del funcionamiento de los dispositivos y las redes digitales.[8]

Esta definición es común a muchos autores. La intrusión e interrupción pueden ser parte de actividades patrocinadas por Estados, incluyendo sabotaje y espionaje. Sin embargo, los Estados están lejos de ser los únicos actores que realizan intrusiones e interrupciones. Cibercriminales con motivaciones económicas probablemente representan la gran mayoría de la intrusiones, mientras que una amplia gama de actores no estatales regularmente interrumpen las actividades digitales.[9]

Como esta definición es más limitada que algunas otras, agregamos dos salvedades importantes. Primero, esta definición no incluye las amenazas ni los riesgos generales planteados por las tecnologías emergentes, tales como la inteligencia artificial (IA), a menos que tales tecnologías se usen para facilitar o amplificar las intrusiones e interrupciones.[10] La IA, incluida la generación de contenido en textos, imágenes o videos "deepfakes", por sí misma no es un problema de ciberseguridad.

Segundo, esta definición no incluye las preocupaciones sobre contenido. La cuestión de si la diseminación de contenido no deseable en línea es un problema de ciberseguridad ha sido debatido históricamente. Muchos expertos han comentado sobre la división entre los que apoyan perspectivas "afines" (o "multiactor") en ciberseguridad, quienes no incluyen las preocupaciones de contenido en su concepción de la ciberseguridad, y los oponentes de este punto de vista, agrupados de manera general y simplista bajo el término "cibersoberanía".[11] Sin embargo, esta división se ha reducido en años recientes pues los Estados "afines" han priorizado las preocupaciones de contenido bajo la etiqueta "desinformación" u "operaciones de influencia/información".[12]

Hay traslapes entre las preocupaciones sobre el contenido y la interferencia maliciosa según se definió anteriormente, sobre todo en las operaciones de "hackeo y filtración".[13] En consecuencia, en este informe incluimos los asuntos de contenido que se relacionan al género, tal como la "pornovenganza" (la publicación sin consentimiento de fotos o videos íntimos), en los cuales hay un elemento de interferencia maliciosa para la obtención de dicha información.[14]

A pesar de estos traslapes, reconocemos que los temas antes citados – la IA,[15] los

deepfakes[16] y la desinformación[17] – tienen impactos en cuanto al género. Asimismo, el troleo, la intimidación y el acoso en redes sociales claramente tienen impactos de género y son un problema social y político urgente.[18] Aunque estos temas son vitalmente importantes, no necesariamente conllevan una interferencia maliciosa mediante dispositivos y redes digitales, por lo cual no se analizan aquí.

Nuestra definición de ciberseguridad por sí misma tiene implicaciones en cuanto al género,[19] pues se deriva de la seguridad de redes, dispositivos y sistemas, en vez de los individuos de identidades y expresiones de género y sexuales marginalizadas (y otros grupos minoritarios). Empezar con el individuo – particularmente las mujeres – es sumamente eficaz para demostrar la relevancia de las tecnologías digitales para las dinámicas y jerarquías de género existentes. No obstante, es menos eficaz para demostrar las maneras en que elecciones "técnicas" supuestamente neutras ante el género – en el diseño tecnológico, las prácticas cotidianas y la regulación – son, de hecho, en sí mismas desarrolladas sobre jerarquías, supuestos e inequidades de género (y a menudo, sin advertirlo, producen otras nuevas). Por lo tanto, empezamos con este elemento más técnico de la ciberseguridad y trabajamos hacia afuera para examinar sus supuestos sobre género y sus efectos sobre los individuos.[20] Al hacerlo así, esperamos hablarles a las y los actuales creadores de

El género informa la ciberseguridad de dos maneras claves.

Primero, el género construye identidades individuales, roles y expectativas de género dentro de la ciberseguridad y en la sociedad en general, tal como la frecuente asociación de la experticia con los hombres y la masculinidad. Segundo, el género opera como una forma de estructura social jerárquica. Esto a menudo, pero no siempre, significa que las actividades y los conceptos asociados con la masculinidad, como la experticia técnica, se valoran más que los asociados con las mujeres y la feminidad, tal como la experticia sobre políticas o iniciativas de equidad y diversidad.[21]

políticas de ciberseguridad y profesionales en un lenguaje que les sea familiar, revelar las implicaciones en cuanto al género de las supuestamente tecnologías y prácticas neutras ante el género y ayudar a personas profesionales y creadoras de políticas a desarrollar sus propias perspectivas de género.

2.1 El marco de tres pilares

El marco para analizar el género y la ciberseguridad que usamos en este informe tiene tres pilares.

Pilar 1. Diseño.

El pilar de diseño de la ciberseguridad pretende construir seguridad dentro de los sistemas socio-tecnológicos. Esto reduce el área superficial de ataque y previene clases enteras de vectores de vulnerabilidad o ataques. También incentiva o requiere que los individuos y las organizaciones actúen en maneras que aumenten, en vez de que disminuyan, su seguridad. Este pilar procura prevenir y mitigar la interferencia maliciosa de manera bastante anticipada, generalmente modelando amenazas y diseñando contra esos modelos.

Pilar 2. Defensa.

Como lograr un diseño de ciberseguridad "perfecto" es imposible, el pilar de defensa tiene que ver con las estrategias para reducir el riesgo, identificar vulnerabilidades y mitigar los daños potenciales después de que los sistemas hayan sido diseñados e implementados. El pilar de defensa de la ciberseguridad aspira a anticipar, detectar, identificar y neutralizar amenazas más específicas de interferencia e interrupción de los dispositivos y las redes digitales.

Pilar 3. Respuesta.

Como la defensa de la ciberseguridad es una cuestión de gestión de riesgos, siempre habrá incidentes de ciberseguridad: intrusiones e interrupciones exitosas de los dispositivos y las redes digitales. Este último pilar de la ciberseguridad se refiere a cómo los Estados responden a estos incidentes. Esto incluye la investigación y recuperación post incidente, las medidas legales para sancionar y disuadir a los infractores, limitar la

diseminación de los incidentes mediante el intercambio de información y la compensación a los afectados. Este marco se alinea muy de cerca con las concepciones prevalentes de ciberseguridad en las comunidades de profesionales y personas expertas. Estas comunidades generalmente ven el propósito de la ciberseguridad como la prevención de intrusiones e interrupciones, en línea con la definición limitada de ciberseguridad antes mencionada.[22] Además, estos tres pilares resuenan con los conceptos comunes usados en estas comunidades, tal como "seguridad por diseño" (pilar 1), medidas de "defensa de la ciberseguridad" (pilar 2) y "respuesta a incidentes" (pilar 3). Esperamos que la estructura cíclica del "flujo de trabajo" de estos pilares – pasar del diseño mediante la defensa a la respuesta (y de vuelta al (re)diseño) – sea intuitiva a las personas profesionales que utilizan marcos similares y priorizan sus planes y operaciones.

Este amplio marco tiene el propósito de ser exhaustivo, en el sentido de que todas las acciones de ciberseguridad calzan en por lo menos uno de estos pilares. Dada su simplicidad, hay áreas de traslape. No siempre es fácil decidir dónde termina el diseño y empieza la defensa, pues la mayoría de la defensa confrontativa de la ciberseguridad (que protege blancos particulares contra agentes de amenaza específicos) puede ser asistida e incluso considerada superflua gracias a un buen diseño de la ciberseguridad. La defensa y la respuesta también se traslapan entre sí porque – como ilustra la bien conocida "cadena de exterminio" de la ciberseguridad – la intrusión e interrupción cibernética es un proceso con múltiples etapas, y cada etapa se puede abordar por separado.[23]

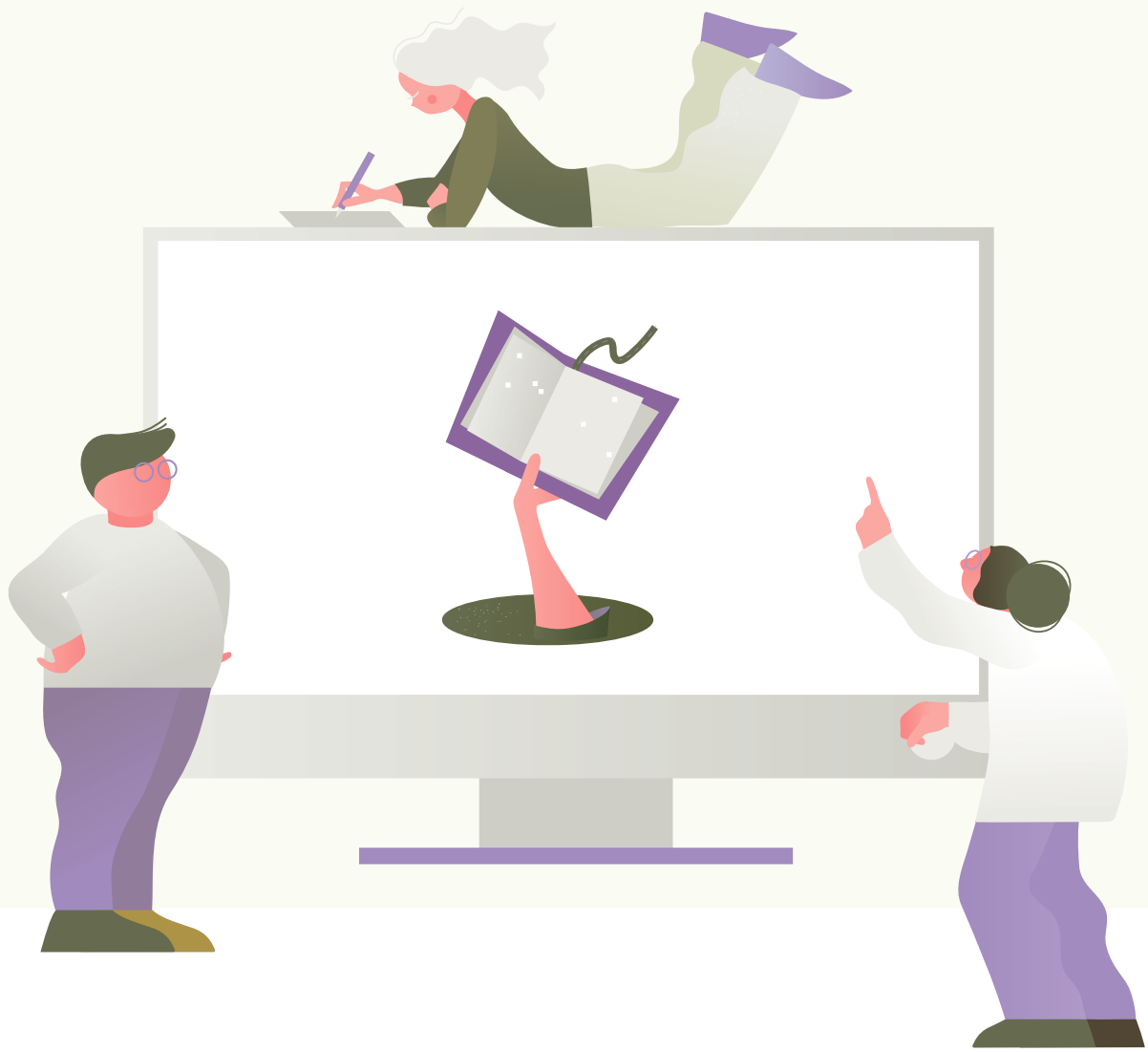
Finalmente, el marco de tres pilares combina la implementación de normas y el desarrollo de capacidades. El desarrollo de capacidades, incluida la capacidad de la ciberseguridad estatal y no estatal, implica mejoras en todo el diseño, la defensa y la respuesta, mientras que las 11 normas de conducta responsable de los Estados avaladas por la Asamblea General de las Naciones Unidas por consenso en el 2015 también pueden implementarse mediante acciones en el diseño, la defensa y la respuesta de la ciberseguridad.[24]

En los capítulos siguientes, proveemos una perspectiva de género sobre cada uno de los pilares de la ciberseguridad enfocándonos en tres casos de estudio: las normas de ciberseguridad, el talento y la experticia y las medidas legales (vea la Tabla 1). Los casos de estudio fueron escogidos porque captan la investigación y la política existente sobre género, ofrecen la oportunidad de presentar recomendaciones específicas a los procesos actuales de ciberseguridad y son claves para la implementación de las normas y el desarrollo de capacidades.

Tabla 1. Marco de tres pilares de la ciberseguridad

Pilar	Caso de estudio	Otros elementos (ejemplos no exhaustivos)
Diseño	Normas	Investigación Modelado de amenazas Desarrollo de guías amigables con las personas usuarias
Defensa	Talento y experticia	Preparación y protección Monitoreo de amenazas Seguro y responsabilidad
Respuesta	Medidas legales	Respuesta a incidentes Intercambio de información (para mitigación) Seguro y compensación

3. Diseño



Más allá del contexto específico de la ciberseguridad, el diseño de la tecnología es sesgado en cuanto al género: malinterpreta, omite y consolida ciertos usos sesgados en cuanto al género, privilegia las prácticas que se conciben como masculinas por encima de las femeninas y esencializa la feminidad en formas problemáticas.[25] Estos aspectos sesgados en cuanto al género tienen impacto directo sobre la ciberseguridad. Muchas personas diseñadoras de tecnología están conscientes de las implicaciones sesgadas en cuanto al género de su trabajo, y hay subdisciplinas completas, incluyendo la experiencia de personas usuarias y el diseño centrado en personas usuarias, que esperan mejorar el diseño de la tecnología con base en género.[26] A continuación presentamos algunos ejemplos seleccionados de diseño de tecnología sesgado en cuanto al género:

- Los prototipos de realidad virtual, como muchas tecnologías, han omitido a las mujeres casi en su totalidad como usuarias meta.[27]
- Se ha demostrado que la elección de las mujeres para asistentes de voz de teléfonos, parlantes y dispositivos inteligentes y la navegación satelital refuerza prejuicios nocivos sobre las relaciones de poder con base en el género.[28]
- El diseño de tecnologías comercializadas directamente hacia las mujeres, conocida como "femvertizing", a menudo "se alimenta de la supuesta necesidad de las mujeres de corregir comportamientos problemáticos o anomalías físicas inaceptables".[29] Los supuestos sesgados en cuanto al género sobre lo que es "normal" se utilizan en los materiales publicitarios para alentar a las mujeres a comprar productos que les permitan someterse o minimizar las características físicas y personales "anormales".
- Hay diferencias en cuanto al género en la investigación académica y de la industria sobre la tecnología, como en otros campos, que incluye las prácticas sobre cómo citar.[30]

Estos aspectos sesgados en cuanto al género más amplios del diseño de la tecnología influyen en la ciberseguridad de varias maneras. A nivel más básico, la concepción de ciberseguridad empleada en el diseño tecnológico es sesgado en cuanto al género. Por ejemplo, el diseño de los dispositivos para el hogar inteligentes no ha incluido adecuadamente la violencia de pareja en la fase de diseño del 'modelado de amenazas', lo cual lo cual significa que los supuestamente seguros dispositivos inteligentes aumentan los riesgos relacionados con el género.[31]

Incluso los servicios diseñados para evitar este problema, tales como los recursos en línea sobre cómo alejarse de relaciones abusivas, pueden en sí mismos ser un riesgo para

las personas si el abusador descubre la herramienta. Por ello, las y los diseñadores de tales herramientas – tales como botones de "salida" de emergencia en las páginas web de organizaciones de víctimas – tienen que tomar en cuenta estos riesgos en sus modelos de amenazas.[32] Para reducir la ocurrencia de estos puntos ciegos peligrosamente pasados por alto es importante que el diseño y los procesos de modelado de amenazas incluyan perspectivas diversas y personas de grupos minoritarios.[33]

Otro ejemplo puede encontrarse en las medidas contemporáneas de ciberseguridad que pretenden proteger a personas de las invasiones a la privacidad o el robo de identidad, las cuales dependen del uso de información personal para el respaldo de contraseñas y acceso a las cuentas en línea. Estas asumen que los "malos" son extraños sin otro acceso al segundo nombre de uno de los padres o al nombre de la primera mascota – un supuesto que no cumple en casos de violencia de pareja o violencia intrafamiliar.[34] El diseño de los procedimientos de verificación de identidad en línea, por ende, tienen efectos en cuanto al género debido a la concepción de "amenaza" que utilizan (y, en este caso, omiten).

La carga de la ciberseguridad también es condicionada por el género. Los ajustes de privacidad en las redes sociales tienen mayor probabilidad de ser activados por mujeres, especialmente para resguardar las imágenes.[35] Se espera que las mujeres ejerzan un control casi absoluto sobre su propia huella digital (por ejemplo, cambiando contraseñas y borrando cuentas de redes sociales, etc.) con el fin de reducir su vulnerabilidad al control coercitivo digital.[36] El no actuar como una usuaria digital perfecta – debido a falta de tiempo o alfabetización o la dependencia en la tecnología para obtener apoyo y conexiones sociales – se vuelve una fuente para responsabilizar a la víctima.[37] Las diferentes metas de la ciberseguridad también se neutralizan entre sí: por un lado, permitir a las empresas diseñar aplicaciones con acceso a la ubicación y otros datos pueden ser una manera de prevenir otras amenazas a la privacidad, mientras que el uso comercial que hacen las compañías de estos datos puede ser una amenaza en sí.

Finalmente, la publicidad sobre las tecnologías de ciberseguridad es sesgada en cuanto al género. El software que puede monitorear teléfonos y otros dispositivos remotamente está marcadamente diseñado para la protección de los y las menores de edad al permitir a las familias rastrear los movimientos de sus hijos e hijas en línea.[38] Pero este software también es usado en situaciones de violencia de pareja (con frecuencia se llama "stalkerware").[39] Google ha prohibido toda publicidad sobre estas aplicaciones espía para

combatir el problema de su uso dual.[40]

En general, el diseño de la ciberseguridad hereda las omisiones y los sesgos en cuanto al género y el refuerzo de los supuestos sobre género que son evidentes en el diseño de la tecnología. Los modelos de amenazas, los procedimientos de notificación y control de personas usuarias y la publicidad de las tecnologías de ciberseguridad significan que las mujeres (o los grupos de género más vulnerables en un contexto en particular) tienen más probabilidad de restar importancia a las amenazas u omitirlas, más probabilidad de tener cargas adicionales de seguridad y más probabilidad de ser afectadas por el mercadeo engañoso sobre ciberseguridad.

3.1 Caso de estudio: las normas de ciberseguridad

El diseño y la implementación de la ciberseguridad se rigen por un amplio rango de normas directas e indirectas que pretenden hacer que las tecnologías digitales sean compatibles con objetivos de calidad, ética, seguridad, integridad, disponibilidad y sostenibilidad, entre otros.

Una norma provee "reglas, lineamientos o características para actividades o sus resultados, con el fin de alcanzar el grado

Sensible al género e inclusivo

Las políticas y los programas sensibles al género reconocen y atienden las diferencias de género en la manera en que las políticas afectan a las personas. La generación de políticas inclusivas en cuanto al género se refiere al uso de lenguaje, procedimientos para la toma de decisiones y otras prácticas que proactivamente apoyan la participación equitativa e influencia de personas de todas las identidades y expresiones de género.[46]

óptimo de orden en un contexto dado".[41] Las normas, como documentos sumamente codificados pero voluntarios, son un punto medio entre los reglamentos técnicos obligatorios y las "mejores prácticas" generales.[42]

Las normas abarcan una amplia gama de temas en los tres pilares de nuestro marco. Sin embargo, la creación de las normas es en sí parte del proceso de diseño que procura estructurar entornos más amplios de ciberseguridad en vez de defender contra amenazas específicas o responder a ellas.

Las normas específicas de ciberseguridad son tanto públicas como privadas y son propuestas por una variedad de entidades: órganos nacionales de normas tales como el National Institute of Standards and Technology (NIST) de Estados Unidos; organizaciones internacionales como la Organización Internacional de Normalización (ISO), la Comisión Electrotécnica Internacional (CEI) y la Unión Internacional de Telecomunicaciones (UIT); entes reguladores técnicos tales como la Internet Engineering Task Force (IETF) o asociaciones específicas a una industria o sector u organizaciones no gubernamentales de defensoría.[43]

Los organismos internacionales de normalización han reconocido que necesitan ser "sensibles al género", o sea,

Análisis de género

El análisis de género requiere la recopilación sistemática y el análisis de datos empíricos sobre las diferencias de género y las relaciones sociales en contexto con el fin de identificar y entender las inequidades y estructuras sociales basadas en género (y otras formas importantes de poder social y cultural). Es la base de la creación de políticas sensibles al género.[50]

estar conscientes de los impactos diferenciados según el género, e incluir la "perspectiva de género", o sea, utilizar un proceso para la generación de normas que incorpore diferentes perspectivas de género, aborde las desigualdades de género e idealmente empodere a las mujeres y niñas.[44] La UIT creó su Grupo de Personas Expertas sobre Mujeres en la Normalización como parte de sus esfuerzos para lograr el objetivo 5 de los Objetivos de Desarrollo Sostenibles (ODS) sobre igualdad de género y empoderamiento de las mujeres.[45]

En el 2019, la Comisión Económica de las Naciones Unidas para Europa (CEPE) publicó una declaración sobre "Normas sensibles al género y desarrollo de las normas", firmada por más de 50 organizaciones de normalización. Esta delineaba tres grupos de acciones:

1. trabajar hacia entornos de preparación de normas balanceados en cuanto al género, representativos e inclusivos;
2. crear normas sensibles al género y
3. crear órganos de normas sensibles al género.[47]

Después de dicha declaración, la ISO preparó un Plan de Acción sobre Género que incluye la participación en la generación de las normas, participación en los órganos de normalización y contenido en las normas sensible al género.

Estas iniciativas proveyeron un enfoque más estructurado hacia la investigación existente sobre los impactos de las normas en cuanto al género. Algunos ejemplos canónicos de revisión de las normas luego del análisis de género incluyen normas de seguridad para los automóviles (cuyos cinturones de seguridad y pruebas de colisión están diseñados para el peso y tamaño promedio del cuerpo de los hombres) y las normas de eficiencia del aire acondicionado de las oficinas (que se basaban en las tasas metabólicas de los hombres y subestimaban de manera significativa el metabolismo de las mujeres).[48] La investigación también ha identificado otras normas, especialmente las relacionadas con los ODS de las Naciones Unidas, tales como las cadenas de abastecimiento de textiles o los equipos de cocina no contaminantes que tienen impactos diferenciados sobre las mujeres debido a que su rol en estas actividades es mayor y a que pasan un tiempo desproporcionado en ellas.[49]

Para considerar las implicaciones sobre el género de las normas de ciberseguridad, nos

enfocamos en la serie 27000 preparadas por la ISO y la CEI y publicadas en dos iteraciones, en el 2005 y en el 2013.[51] Las serie ISO 27000 es una familia de normas de gestión de la seguridad de la información que se apoyan unas a otras y que "pueden combinarse para brindar un marco reconocido globalmente para la gestión de la seguridad de la información con base en las mejores prácticas".[52] Usamos el ejemplo de la ISO debido a su influencia global y amplio reconocimiento, aunque la discusión podría aplicarse de igual manera a otras normas y organizaciones.[53]

Es difícil evaluar la participación en cuanto a género en el desarrollo histórico de la serie ISO 27000 pues incluye asesoría y consulta externa. El actual comité de ISO 27000, sin embargo, está empezando a recopilar datos sobre el número de hombres y mujeres que participan en los diversos proyectos de dicho comité, incluyendo las ratios absolutas de hombres y mujeres en diferentes roles y a diferentes niveles (por ejemplo, editores de proyectos) y las distribución geográfica y nacional de sus miembros.[54]

Este análisis de género de participación en la elaboración y gestión de la serie ISO 27000 es vital pues procura garantizar que se reconozca un rango diverso de puntos de vista en la creación de las normas y en la gestión y operación de las organizaciones de normalización. Sin embargo, es solo el primer paso. Luego de la amplia definición de igualdad de género presentada anteriormente, los análisis futuros deberían considerar si la participación es significativa y eficaz en la implementación del cambio.[55]

Asimismo, los esfuerzos para analizar (y, de ser necesario, ampliar) la participación tienen que estar acompañados de un análisis de género del contenido de las normas. Hasta ahora, las normas de ciberseguridad ISO 27000 han estado dominadas por el supuesto de que son genéricas y, por lo tanto, neutras en cuanto al género, en línea con las tendencias generales en el diseño tecnológico mencionados anteriormente.

Las personas interesadas en la ISO sí mencionaron un ejemplo de lenguaje sesgado en cuanto al género en la serie 27000 que posteriormente fue cambiado. Hace varios años, el término "housekeeping" [quehaceres domésticos] fue señalado por las mujeres que participaban en la discusión de la revisión de las normas como inapropiado debido a sus connotaciones en cuanto al género: aunque, en la ciberseguridad, housekeeping [administracion interna] se refiere al proceso de optimización del espacio en el disco duro, fuera de la ciberseguridad, housekeeping es una categoría de trabajo feminizado que con frecuencia es subvalorado u omitido de los análisis de empleo.[56] El término fue removido posteriormente y reemplazado por un lenguaje más neutro.[57] Un análisis

completo del contenido de la serie 27000, incluido no solo el lenguaje sesgado en cuanto al género sino los efectos con respecto al género (por ejemplo, mediante supuestos sobre personas usuarias y riesgos relevantes) podría identificar ejemplos adicionales.

El trabajo actual sobre la serie 27000 también resalta que la preparación de normas tiene que abordar asuntos tanto de contenido como de participación con el fin de volverse sensible al género. Estas vías podrían coordinarse con el Plan de Acción sobre Género general de la ISO. Las normas ISO se someten a revisiones cíclicas cada tres años, en las cuales pueden incorporarse las recomendaciones nuevas basadas en género. Las normas ISO también pueden ser revisadas antes si se identifica un tema urgente.

3.2 Áreas adicionales a investigar

Un tema importante a investigar en el futuro tiene que ver con las maneras de abordar los impactos potenciales en cuanto al género en las normas de ciberseguridad. Estos incluyen la violencia basada en género facilitada por los dispositivos para el hogar conectados a la Internet[58] y el efecto desproporcionado de las filtraciones de datos sobre hombres y mujeres.[59]

Aunque la ciberseguridad en las cadenas de suministro de tecnología ha recibido bastante atención,[60] es posible que las normas de ciberseguridad sobre las cadenas de suministro "limpias" (o sea, aquellas que no introducen código malicioso ni aumentan el riesgo de interferencia maliciosa) también tienen impactos indirectos sobre el género debido a la participación de hombres y mujeres en las ocupaciones relevantes (por ejemplo, en las fábricas de microchips).

Otra área importante que requiere mayor investigación se relaciona con la integración de normas de ciberseguridad sensibles al género en la investigación y las políticas sobre los protocolos básicos de Internet. Como parte de los esfuerzos generales para abordar los impactos sobre los derechos humanos de los protocolos de Internet en el IETF,[61] varios documentos han sugerido que es necesario realizar un análisis de género.[62] Estos debates sobre la "neutralidad" de los protocolos de Internet podría aplicarse positivamente a las normas de ciberseguridad para que sirvan como ejemplos de cómo – y cómo no – incorporar las consideraciones de género en los entornos técnicos.

3.3 Recomendaciones

- Las organizaciones internacionales de normalización, en cooperación con los organismos nacionales de normalización, deben identificar y recopilar datos sobre las áreas en las cuales las normas de ciberseguridad tienen efectos en cuanto al género.
- Con base en los datos recopilados y su análisis, deben revisarse la normas de ciberseguridad actuales en una manera que sea sensible e inclusiva con respecto al género.
- Todas las propuestas nuevas de normas de ciberseguridad deben estar sujetas a una evaluación de impacto sobre el género para garantizar que sean sensibles e inclusivas en cuanto al género. Las y los profesionales deben recibir capacitación sobre género y ciberseguridad para apoyarles en la conducción de estas evaluaciones.
- Las organizaciones internacionales de normalización y los organismos nacionales de normalización deben asegurarse de que todos los grupos de trabajo que están preparando normas de ciberseguridad incluyan personas expertas en igualdad de género e interseccionalidad.
- Las organizaciones internacionales de normalización y los organismos nacionales de normalización deben asegurar representación diversa en cuanto al género en los procesos de creación de normas de ciberseguridad, en las consultas con partes interesadas y dentro de la organizaciones de estandarización mismas.

4. Defensa

La manera en cómo pensamos sobre la defensa, o sea, qué significa defender y las acciones de sentido común que tomamos para defender, es sesgada en cuanto al género. Refleja una serie de normas asociadas con la masculinidad (por ejemplo, protección, competencia técnica, autonomía, etc.) que se derivan de la manera en que los militares entienden la seguridad nacional.[63] A menudo esto es positivo porque hace que la ciberseguridad sea inteligible para un gran rango de personas no expertas mediante el uso paralelo de conceptos y lenguaje.

Sin embargo, también puede tener efectos negativos. Muchos de los desafíos asociados con el género y la defensa de la ciberseguridad se derivan de una incongruencia entre el entendimiento convencional de la defensa nacional y la ciberseguridad, el cual se basa en la premisa de mitigar y gestionar, en vez de eliminar, los riesgos. Las normas y expectativas masculinas que se relacionan con el uso de la fuerza para producir seguridad física, por ejemplo, pueden llevar a las personas creadoras de políticas a subestimar los daños no físicos en la ciberseguridad.[64]

Las normas del género masculino sobre la vulnerabilidad pueden hacer que admitir un error, buscar ayuda o trabajar en colaboración sea más difícil.[65] Esto puede llevar a renuencia a buscar activamente la defensa de la ciberseguridad o a ser lo suficientemente transparente sobre las fallas con clientes, empleados o ciudadanos. Tales normas también pueden llevar a priorizar algunas personas y organizaciones – que a menudo se consideran socialmente prestigiosas o valiosas para la defensa y protección (tal como el Estado, las fuerzas armadas o las grandes corporaciones) – por encima de otras (tales como las organizaciones y personas de la sociedad, notablemente mujeres y personas LGBTQ+[66]).[67] Una perspectiva de género plena sobre la defensa de la ciberseguridad reconoce que las sociedad civil y los grupos que representan a las mujeres y las personas LGBTQ+ tienen necesidad y derecho a la defensa de la ciberseguridad, incluyendo los recursos que los Estados (en términos de desarrollo de capacidades, experticia y cumplimiento) necesitan para proporcionarlos.

Más concretamente, diferentes elementos de la defensa de la ciberseguridad plantean problemas de género separados. Las amenazas deben monitorearse mediante la evaluación y el análisis continuos de las redes, la infraestructura y los dispositivos para detectar intrusiones potenciales o interrupciones deliberadas.[68] A consecuencia de esto, a nivel básico, lo que se considera una amenaza está sesgado en cuanto al género. La ciberseguridad por lo general se interesa de la seguridad militar y corporativa (y, por ende, se relaciona con el espionaje y el robo económico). No obstante, un

entendimiento basado en género de las amenazas a la ciberseguridad reconoce que aquellas amenazas "tradicionales", tal como los ataques de denegación de servicio a los servicios de los Estados, tienen resultados relacionados con el género.[69] También reconoce que la violencia íntima de la pareja, el doxeo, el ciberacoso y la distribución sin consentimiento de imágenes íntimas (o sea, la "pornovenganza") también son amenazas que pueden provenir de la intrusión o interrupción de los dispositivos y redes personales.[70]

En lo que respecta a los procesos técnicos, hasta el momento el monitoreo de amenazas depende del aprendizaje automático que es vulnerable a importar los problemas de género presentes en el campo del aprendizaje automático, incluyendo los supuestos y datos sesgados en cuanto al género incorporados en los algoritmos.[71] Incluso este proceso automatizado en gran medida depende del juicio de seres humanos sobre las prioridades organizacionales, la distribución de recursos y el desarrollo de capacidades – abriendo todas ellas el potencial para la creación o intensificación de desigualdades. Por ejemplo, un filtro automático de correo electrónico que identifica mensajes potencialmente peligrosos debería alertar sobre las estafas románticas además de los mensajes de phishing y las estafas financieras.[72]

Los procesos de preparación y respuesta ante las amenazas también son sesgados en cuanto al géneros. Las simulaciones de amenazas, por ejemplo, tales como la práctica común de enviar mensaje electrónicos falsos de phishing, a menudo involucran estereotipos de género (por ejemplo, una mujer en un puesto de asistente, un hombre como Director General).[73] Hacen falta datos desagregados por género sobre las víctimas de phishing, lo que hace que las consecuencias del phishing con respecto al género sean difíciles de evaluar.

Pero tal evaluación es esencial pues, si muchos fallos de la ciberseguridad son producto de error humano, las personas creadoras de políticas necesitan tener una variedad de enfoques hacia el "ser humano" que está cometiendo los errores.

Los programas de recompensa de errores (bug bounty programs), que abarcan un amplio espectro de maneras en que hackeadores "amistosos" identifican las vulnerabilidades y respuestas de defensa de una organización mediante vectores digitales, sociales o físicos tienen problemas asociados. Como estas contiendas están diseñadas para ser anónimas, solo se conocen los seudónimos (o sea, los alias de los hackeadores) de los cazadores de recompensas más prolíficos y sus pagos. Las

consecuencias de esta anonimidad no están claras: podría hacer que sea más fácil que las mujeres y las personas LGBTQ+ participen o podrían agravar las desigualdades de género de la ciberseguridad y la cultura de hackeo en general (vea el caso de estudio a continuación). Además, la caracterización de las amenazas mismas, desde la popular imagen de hackeadores encapuchados que usan los medios de comunicación hasta los nombres y las fotos usados en los informes técnicos de ciberseguridad, a menudo incluye cualidades sesgadas en cuanto al género y estereotipos nocivos.[74]

Finalmente, los intentos de proteger a las organizaciones (y, en cierta medida, a los individuos) de los costos y peligros provenientes de los ataques a la ciberseguridad, predominantemente por medio de pólizas de seguro de ciberseguridad, también deberían ser evaluados para determinar sus implicaciones en cuanto al género.[75] Como con todo seguro, es importante que las evaluaciones de las amenazas incluyan un análisis de género, que los criterios de elegibilidad para un seguro puedan ser cumplidos por mujeres, hombres y personas no binarias y que los precios para organizaciones e individuos no dependan de estereotipos de género ni produzcan resultados discriminatorios basados en el género.[76]

4.1 Caso de estudio: talento y conocimiento

El talento y la experticia son temas ampliamente reconocidos en la industria de la ciberseguridad. Aunque la cuestión del talento y experticia obviamente tiene que ver con todos los aspectos de la ciberseguridad, nos enfocamos acá en la práctica de la "defensa" (o sea, la implementación de la seguridad) pues esta generalmente se entiende como la actividad central de la ciberseguridad.

Los problemas relacionados con el talento y la experticia con frecuencia se expresan como una "brecha" en las competencias en ciberseguridad, lo que significa que el número de puestos disponibles es mayor que el número de personas calificadas para ocuparlos.[77] Según lo demuestra la investigación realizada por organizaciones como el Global Forum on Cyber Expertise, esta brecha de talento es mundial, aunque las presiones se expresan de manera diferente en diferentes contextos locales.[78] Muchos Estados han tomado pasos para motivar a las personas a unirse a la industria de la ciberseguridad y mejorar el nivel de sus destrezas una vez ahí. Esto frecuentemente se complica debido a la presión competitiva entre los gobiernos y el sector privado, pues los puestos en los gobiernos luchan por competir con los salarios en el sector privado.[79]

Estos problemas con el talento y la experticia se agravan debido a la desigualdad, los peligros y la visibilidad en cuanto al género. Debido a las limitaciones de espacio, esta sección discute estas dinámicas de manera bastante general. Sin embargo, entender cómo y por qué las brechas, las inequidades y los peligros basados en el género operan en contexto requiere un análisis de género interseccional que examine cómo el género, la raza, la sexualidad, la clase y la ubicación urbana o rural, entre otros factores, interactúan para apoyar la participación de algunos grupos en los campos de la informática mientras marginalizan a otros.

Una encuesta reciente del International Information System Security Certification Consortium indica que un 24 por ciento de las personas profesionales en ciberseguridad en el mundo son mujeres.[80] El Estudio Mundial sobre la Fuerza Laboral en la Seguridad de la Información del 2017 determinó que esta falta de representación estaba acompañada de diversas formas de desigualdad y que el 87 por ciento de las mujeres reportaron discriminación inconsciente y un 19 por ciento discriminación manifiesta.[81] Este es un problema ampliamente reconocido, con muchas páginas web y cuentas en redes sociales que crean redes de "mujeres en ciberseguridad" y eventos específicamente dirigidos a mujeres.[82]

También existen eventos, redes e iniciativas de desarrollo de capacidades similares para apoyar la igualdad, equidad y participación de las personas queer en ciberseguridad.[83] Debido a las críticas por la falta de representación y visibilidad en las conferencias de ciberseguridad,[84] eventos como la Conferencia RSA – una prestigiosa serie de eventos internacionales de tecnologías de la información (TI) – han procurado garantizar la paridad de género entre los ponentes principales y aumentar la participación de las mujeres en general.[85]

Dividimos los temas de género en talento y experticia en ciberseguridad en tres áreas separadas: la dinámica de género en general en las profesiones de ciencias, tecnologías, matemáticas e ingeniería (STEM), el género en la informática y codificación y el género en la industria de ciberseguridad específicamente. Reconocemos que no todos los puestos en ciberseguridad son puestos STEM o "técnicos"; la prominencia de estos puestos en ciberseguridad refleja una valoración sesgada en cuanto al género de los trabajos entendidos como "masculinos" por encima de otros. Estos puestos, no obstante, también reflejan dónde las disparidades de género son más evidentes, y por ello nos enfocamos en estos puestos en esta sección.

4.1.1 La dinámica del género en STEM

Los temas de género en las profesiones STEM – repetimos, entendidos como una "brecha de género" entre hombres y mujeres – han sido bastante investigados y generalmente se entienden en términos de participación [pipeline] y retención.[86] Debe mencionarse que mucha de esta investigación y política utiliza un entendimiento binario, a menudo heteronormativo del género; es necesario hacer mucho más para entender las experiencias y el apoyo de la participación equitativa de personas no binarias y queer en STEM y ciberseguridad. Las causas de la "brecha de género" son complejas y específicas al contexto. Por lo general, las barreras a la igualdad de género en STEM incluyen (a) disparidades en el acceso a infraestructura y educación; (b) limitaciones financieras y prioridades a nivel individual y familiar y (c) la persistencia de normas de género socioculturales e institucionales que sugieren que las profesiones STEM predominantemente son para hombres.[87] En algunos contextos, tales como Malasia y Oriente Medio, la participación de las mujeres en educación en STEM es considerable pero no se traduce a carreras en STEM.[88] En Estados Unidos de América y el Reino Unido, por el contrario, sigue siendo menos probable motivar a las niñas a estudiar materias relacionadas con STEM y menos probable que consideren que tienen talento o experticia en STEM.[89]

Muchas de las políticas orientadas a aumentar la participación de las mujeres en STEM también se han aplicado a la industria de la ciberseguridad. Estas incluyen mayor incorporación de destrezas de STEM en la educación de las niñas,[90] promoción de programas universitarios sobre STEM entre niñas y mujeres,[91] reclutamiento activo de mujeres mediante visitas a centros universitarios y campañas en las redes sociales,[92] ofrecimiento de mentorías y educación continua a mujeres y niñas que ya están trabajando en organizaciones y cambios en las políticas de recursos humanos para priorizar la contratación y retención de las mujeres (por ejemplo, requiriendo que por lo menos una mujer sea entrevistada para todas las vacantes existentes, mejorando las políticas sobre las licencias de maternidad, etc.).[93] Las disparidades a menudo se encuentran en los puestos de mayor rango en STEM y las empresas de tecnología nuevas y, dado que la ciberseguridad es un campo joven y en rápida evolución, la dinámica en cuanto a género del emprendedurismo es sumamente relevante.[94]

4.1.2 El género en la informática y la codificación

Los campos que involucran de manera central las computadoras y la "codificación" (un

término insatisfactoriamente genérico que abarca una amplia gama de diversas destrezas) tienen problemas de género bien documentados. Aunque, repetimos, difieren según el contexto, existe una brecha de alfabetización digital mundial[95] entre mujeres y niñas y hombres y niños.[96] A nivel global, "327 millones menos mujeres que hombres tienen un teléfono inteligente y pueden acceder a la Internet móvil", aunque las mujeres tienen cuatro veces más posibilidades que los hombres de ser profesionales de TI.[97]

Vale la pena recordar que en sus inicios la computación estaba relativamente abierta a las mujeres y que solo se empezó a considerar como una profesión masculina conforme aumentó su prestigio social debido a su creciente importancia en la economía.[98] La investigación ha demostrado que algunas comunidades en línea organizadas alrededor de la codificación – incluyendo los juegos y el hackeo – presentan una cultura masculinista que enfatiza lenguaje agresivo y enfoques individualistas hacia la resolución de problemas y el dominio técnico, a la vez que desvaloran las características que se perciben como asociadas a la feminidad, tal como la empatía y la expresión de emociones.[99] Estas culturas pueden ser explícitamente misóginas y homofóbicas, refiriéndose a las mujeres principalmente como objetos sexuales y a las personas LGBTQ+ con términos de odio y exclusión.[100]

Como estas comunidades a menudo se consideran como un banco de talento de experticia sobre ciberseguridad, existe el riesgo de que el reclutamiento para la ciberseguridad importe normas antifeministas y excluyentes (o sea,

Esencialismo

El esencialismo es un entendimiento del género que asume que la humanidad está dividida en dos sexos biológicamente distintos – masculino y femenino – y que estos dos sexos determina el comportamiento y las características inherentes de los hombres y las mujeres. Con frecuencia se asocia con perspectivas que asumen que todas las mujeres (y todos los hombres) son iguales y, por lo tanto, tienen iguales intereses, necesidades y capacidades. Esto puede oscurecer diferencias interseccionales importantes entre las mujeres (y los hombres y las personas no binarias) con respecto a raza, clase, sexualidad, casta y habilidad, entre otras cosas. Una perspectiva robusta de género reconoce que, aunque hay patrones empíricos de diferencias entre hombres y mujeres, estos patrones no reflejan características esenciales y, por lo tanto, no son inevitables.[107]

actitudes y prácticas que se oponen y desvalorizan la igualdad de género y la inclusión de raza, étnica y sexual) en el lugar de trabajo.[101] Esto hace que los ambientes laborales sean incómodos (u hostiles) para quienes no siguen la norma.[102] El Estudio Mundial sobre la Fuerza Laboral en la Seguridad de la Información del 2017 determinó que el 51 por ciento de las mujeres en el campo habían experimentado discriminación, en comparación con un 15 por ciento de los hombres.[103]

Esto afecta primordialmente a las mujeres y los grupos marginalizados, pero también puede afectar a los hombres que no se identifican con tales normas.[104] Los lugares de trabajo que no tienen una cultura explícitamente antifeminista podrían estar organizados y funcionar bajo el supuesto de que la mayoría de los trabajadores son hombres y que los valores y las prácticas asociados con la masculinidad son neutros o "normales".[105] Aunque a menudo sin intención discriminatoria o consciente, esto perpetúa la estructura sesgada en cuanto al género de la experticia en ciberseguridad y, por ende, influye en la contratación, las oportunidades de ascenso y la habilidad de determinar políticas.

Cuando las mujeres entran a estos campos, su contribución a menudo se enmarca con referencia a características esencialistas tal como destrezas emocionales y sociales. Aunque estos atributos son positivos, enmarcar las contribuciones de las mujeres predominantemente en términos de, por ejemplo, empatía o solidaridad solidifica los estereotipos de género sin necesariamente aumentar el valor atribuido a los aspectos emocionales, sociales y solidarios de la experticia informática.[106]

Se cree que una mayor presencia de mujeres (y otros miembros de grupos marginalizados) en trabajos de ciberseguridad tiene dos beneficios. Primero, puede contribuir a resolver problemas de manera creativa y a mejorar la gobernanza de las políticas y su implementación mediante la introducción de perspectivas diversas.[108] Segundo, se cree que estas perspectivas llevarán a una perspectiva de género en la ciberseguridad en general.[109] La investigación indica que esto puede ocurrir pero que, sin apoyo, las mujeres y los miembros de otros grupos minoritarios podrían más bien sentir presión de adaptarse a la norma en su lugar de trabajo.[110] La incorporación tokenizada de las mujeres y los miembros de grupos minoritarios, sin reconocer sus contribuciones o en maneras que refuerzan los estereotipos, no contribuye a la participación significativa ni a mayor igualdad.[111]

4.1.3 El género en la industria de la ciberseguridad

Algunos asuntos de género se relacionan específicamente con la industria de la ciberseguridad. Como el campo de la ciberseguridad está creciendo en importancia, influencia y prestigio, la participación de las mujeres en ciberseguridad es un asunto de igualdad y equidad en términos de oportunidades para tener éxito, reconocimiento y potencial de ingresos. Algunas prácticas laborales en ciberseguridad, tal como los requerimientos de jornadas en los Centros de Operación de Seguridad, requieren mayor análisis para evaluar sus implicaciones en cuanto al género. Asimismo, muchos programas de certificación en ciberseguridad requieren sesiones intensas con largas horas lo cual es un modelo de trabajo impráctico para personas (probablemente mujeres) con responsabilidades de cuidado infantil.[112]

De forma más sutil, la promoción de ambientes laborales, culturas institucionales y estilos de gestión que son escépticos de la autoridad tradicional o convencional, aunque a menudo elogiada como una característica de una fuerza laboral innovadora, organizaciones ágiles y un sector socio-tecnológico dinámico, pueden facilitar un entendimiento limitado de la masculinidad (y la discriminación) similar a los campos más generales antes citados.[113] Abordar la "brecha de género" en la experticia en ciberseguridad, por ende, requiere políticas que promuevan la inclusión y participación de las mujeres y la capacitación sobre género para reducir el acoso y la discriminación y apoyar los cambios organizacionales y culturales para valorar una variedad de actividades y capacidades, incluyendo aquellas que usualmente se asocian más con la feminidad.[114]

4.2 Áreas adicionales a investigar

Muchas áreas de género y experticia en ciberseguridad requieren investigación adicional. Los debates sobre STEM y las "brechas de género" digitales deben ser contextualizados (o sea, en países específicos, organizaciones intergubernamentales, corporaciones, etc.) y examinados usando un análisis de género interseccional.

Hay una ausencia particular de datos sobre los obstáculos y las oportunidades que experimentan en la ciberseguridad profesional (y la educación en STEM) las personas no binarias y LGBTQ+, así como también personas de otros contextos minorizados (por ejemplo, según su raza, etnia o religión). Deben priorizarse las políticas que buscan

transformar los obstáculos estructurales, en vez de apoyar a los individuos a tener éxito a pesar de ellas.

Debe también ponerse mayor atención a entender las diferencias en los enfoques, y las experiencias, en el sector privado y el sector público, con respecto al género y la experticia informática. Las estructuras profesionales, los incentivos y las prácticas de contratación difieren entre ambos sectores.[115] Por lo tanto, es importante saber si las dinámicas de género ocurren de la misma manera y considerar si las mejores prácticas podrían ser compartidas entre ellos. En consecuencia, tenemos que preguntar si hay una diferencia en la alfabetización técnica (y, de hecho, en los compromisos con la igualdad de género) de personas expertas privadas y públicas. Debe realizarse investigación similar que compare (en contexto) la penetración en el sector privado de las políticas de igualdad de género en la contratación, la retención y el desarrollo profesional.

4.3 Recomendaciones

- Las organizaciones internacionales, los Estados y los organismos profesionales deben asegurarse de que las políticas para promover la igualdad y equidad de género en la ciberseguridad sean sensibles a los contextos locales y las dinámicas de género. Los Estados, en particular, deben elaborar políticas exitosas similares en STEM en general, incluyendo intervenciones que procuren cambiar los sistemas educativos actuales en vez de simplemente facilitar el éxito en ellos.
- Todas las organizaciones del sector público y del sector privado deben tomar medidas activas para contrarrestar las normas antifeministas y excluyentes de los lugares de trabajo en ciberseguridad y crear un ambiente seguro e inclusivo para todos los géneros mediante capacitación obligatoria sobre género y liderazgo significativo de parte de la alta gerencia.
- Mediante incentivos y regulaciones, los Estados deben instar al sector privado a aceptar las políticas de igualdad de género en el diseño, la contratación y la profesionalización autorregulada.
- Las personas creadoras de políticas en los Estados y a nivel internacional, así como las personas profesionales del sector privado, deben aplicar perspectivas de género para identificar supuestos “predeterminados” (a menudo hombre/masculino) en las políticas y prácticas de la ciberseguridad y revisarlas de acuerdo a esto.
- Todas las organizaciones, pero en especial el sector privado y el de educación, deben actuar para mitigar los estereotipos en las prácticas profesionales y de reclutamiento

evitando asociaciones injustificadas entre las mujeres y las destrezas “más blandas” de la ciberseguridad.

- Las organizaciones educativas, los entes profesionales y regulatorios y empleadores deben promover y apoyar grupos y redes para mujeres, personas no binarias y miembros LGBTQ+ de la comunidad profesional de ciberseguridad. Los Estados y la academia deben recopilar datos sobre las experiencias de las personas LGBTQ+ y no binarias, así como también personas de otros contextos minorizados, en la profesión de ciberseguridad (y la educación en STEM) y crear políticas con base en los resultados.

5. Respuesta

La respuesta a incidentes – las medidas de las organizaciones para manejar las intrusiones en la redes, los ataques, las filtraciones de datos y otros actos cibernéticos maliciosos – está caracterizada por una jerarquía de prioridades. Los estudios han mostrado que la industria de la ciberseguridad reporta ciertas víctimas (organizaciones comerciales, gobiernos), que están asociadas con la seguridad "tradicional" y las actividades de los hombres en la élite, y responde a ellas, de manera desproporcionada, y que tiene un punto ciego en lo que respecta a las amenazas a la sociedad civil y la seguridad humana (por ejemplo, las organizaciones no gubernamentales, las instituciones educativas e individuos en general).[116] Como los centros educativos, las organizaciones no gubernamentales y los individuos en general tienen más probabilidad de preocuparse por problemas de poder social, daño e igualdad, esta priorización tiene efectos en cadena en lo que respecta al género.

La composición, las prácticas esperadas y las horas laborales y la cultura de los equipos de respuesta a incidentes también requieren un análisis de género. Existe alguna evidencia de que los equipos de "soporte técnico", que con frecuencia son la primera línea de respuesta después de un incidente de seguridad, predominantemente están compuestos por hombres, lo que acrecienta la asociación de la experticia técnica con la masculinidad.[117]La composición y cultura de los Equipos de Respuesta ante Emergencias Informáticas (CERT o CSIRT) también es una parte de la respuesta de la ciberseguridad. La investigación indica que los CERT tienen estrategias y características políticas distintivas, especialmente a nivel nacional e internacional, y es posible que estas características incluyan dinámicas de género.[118]

El intercambio de información – el proceso del intercambio confiable de información sobre ataques y otros incidentes de seguridad, vulnerabilidades y prácticas de ciberseguridad – también es una parte esencial de la respuesta a las amenazas de ciberseguridad. Las mismas normas nacionales de defensa masculinas podrían impedir que los Estados y las organizaciones compartan información sobre los ciberataques y las vulnerabilidades de los sistemas.

Los estudios sugieren que "comunidades de confianza" informales son la base de gran parte de la información sobre ciberseguridad que se comparte, en vez de utilizar líneas formales de comunicación entre individuos con roles similares.[119] La informalidad de estas comunidades, y el consecuente sesgo inconsciente que proviene de esto, significa que la participación de mujeres y grupos minoritarios en ellas puede ser menor, incluso cuando se ajusta para las proporciones generales en la industria. La respuesta de la

ciberseguridad también puede demostrar una dinámica desafortunada de sesgo en cuanto al género de culpar a la víctima, en cuanto se responsabiliza a las organizaciones o personas con medidas de defensa de la ciberseguridad o protección de identidad que se consideran "insuficientes" como si "estuvieran pidiendo ser hackeadas", lo que vuelca la responsabilidad hacia la parte que ha sido dañada, en vez del que cometió el daño.[120]

El seguro de ciberseguridad también es una parte importante del pilar respuesta. Aunque no es un sustituto para el manejo adecuado de los incidentes de ciberseguridad, la compensación puede ayudar a recuperar los daños relacionados directamente con un incidente en particular. Las aseguradoras también han sido eficaces en trasladar los tomadores de pólizas hacia la respuesta profesionalizada ante incidentes.[121] Sin embargo, las pólizas de seguros corporativos tienen probabilidad de perpetuar los sesgos de género existentes en el objeto de la ciberseguridad al reflejar y reforzar las jerarquías sesgadas en cuanto al género en la priorización de los blancos de ciberseguridad. El mercado en desarrollo de pólizas de seguro de ciberseguridad para individuos, por otra parte, podría introducir nuevos sesgos en las definiciones del ciberacoso o diferentes niveles de compensación para artículos personales y tarjetas de identidad luego de una exposición a un fraude o el robo de identidad.[122] Finalmente, se requieren datos desagregados por género sobre las demandas de indemnización de seguros y los pagos para determinar si existen prácticas discriminatorias o resultados desiguales.[123]

5.1 Caso de estudio: medidas legales

Los Estados usan diversas herramientas políticas y legales para responder a los actos digitales maliciosos. Estas herramientas incluyen señalar y denunciar públicamente (naming and shaming), sanciones diplomáticas y económicas y justicia penal.

Los marcos legales juegan un papel crucial en facilitar las respuestas de los Estados, tanto ante actos maliciosos entre Estados como ante el delito. Aunque los marcos legales son relevantes para todos los pilares de la ciberseguridad – por ejemplo, pueden ordenar medidas de preparación para la ciberseguridad[124] – la legislación es central al pilar "respuesta". Abarca muchos aspectos de la respuesta de la ciberseguridad desde facilitar el intercambio de información hasta la protección de los investigadores de seguridad que participan en pruebas de vulnerabilidad y detección. Las respuestas legales penales también definen, investigan, procesan y disuaden los actos y actores maliciosos.

Aunque la legislación y las normas internacionales juegan un papel crucial en el mantenimiento de la paz y la seguridad, los Estados son los actores primarios en el abordaje de los incidentes de ciberseguridad en sus "territorios", usando herramientas legales locales. A pesar de la separación actual entre los procesos de las Naciones Unidas que tratan de la ciberseguridad internacional y el cibercrimen, las respuestas de la justicia penal a los comportamientos maliciosos en el ciberespacio y la ciberseguridad internacional obviamente están interconectadas. En este sentido, el informe del 2015 del Grupo de Personas Expertas Gubernamentales de las Naciones Unidas sobre los avances en el campo de la informatización y las telecomunicaciones en el contexto de la seguridad internacional incluye recomendaciones pertinentes. Recomienda como una medida específica para el desarrollo de la confianza que los Estados consideren acuerdos voluntarios para "Cooperar, de manera consistente con el derecho nacional e internacional, con las solicitudes de otros Estados de investigar delitos relacionados con [las tecnologías de la información y las comunicaciones (TIC)] o el uso de las TIC para propósitos terroristas o para mitigar actividades TIC maliciosas que emanen de su territorio".[125] También establecer una norma que invita a la cooperación y asistencia en la mitigación de actividades TIC maliciosas cuyo blanco es la infraestructura crítica.[126]

Las respuestas legales también son cruciales para disuadir a los actores maliciosos y llamarlos a rendir cuentas. Incluso los culpables apoyados por un Estado debería ser llevados ante la justicia; evitar la inmunidad es esencial para abordar la actividad maliciosa en el ciberespacio, sea este un delito o actos de adversarios.[127] Dado el problema de la atribución y la falta del uso real del derecho internacional en la respuesta a las ciberoperaciones,[128] muchos Estados han presentado cargos contra actores conectados a adversarios extranjeros bajo la legislación penal nacional.[129]

Con base en el uso que hacen los Estados de su ley penal local para responder a los actos maliciosos de sus adversarios,[130] consideramos que las respuestas legales penales son cruciales para la ciberseguridad. Esto va más allá del problema del así llamado "cibercrimen". Los procedimientos legales penales para la investigación de delitos informáticos se pueden usar para la investigación de virtualmente cualquier acto criminal. En muchos países, el cumplimiento de la ley y los servicios de inteligencia comparten información y herramientas para la investigación de incidentes de ciberseguridad.

La investigación existente ha demostrado que los incidentes que caen dentro de definiciones más amplias de ciberseguridad que la adoptada acá tienen un impacto en

cuanto al género.[131] Esto es obvio en el caso del acoso y la violencia en línea, donde las mujeres y las personas LGBTQ+ son desproporcionadamente atacadas.[132] También se han identificado varias preocupaciones de género con relación a los apagones de Internet y las filtraciones de datos. El extremismo violento en línea y el tráfico sexual en línea, cuyo blanco son hombres y niños además de mujeres y niñas, también cae dentro de esta categoría.[133] Desafortunadamente, las respuestas legales a los incidentes de ciberseguridad no han abordado estos impactos sobre el género en una manera sistemática, con lo cual han agravado el problemas de que la ley generalmente promueve la "articulación de las inequidades de género".[134]

Los marcos legales típicamente consideran solo los aspectos inmediatamente más obvios de género y ciberseguridad, tales como el acoso y la violencia focalizados directamente contra personas identificables o cometidos por personas identificables. Incluso en estos casos, el género no siempre se incorpora de manera equitativa. Los problemas relacionados con el género obstaculizan el acceso a la justicia y los tribunales, variando de expectativas rígidas sobre conductas "apropiadas" para hombres y mujeres; acceso diferenciado a los recursos materiales y el capital social requerido para procesar un caso; prejuicios relacionados con la credibilidad relativa de hombres y mujeres (particularmente personas LGBTQ+) y recursos diferenciados dedicados a la investigación y el procesamiento de los delitos que usualmente experimentan los hombres en comparación con los experimentados por las mujeres (particularmente las mujeres minorizadas o trans) y las personas no binarias.[135] Los supuestos esencialistas que presuponen que las mujeres son las víctimas[136] y los hombres los infractores contribuyen a procesos de (re)victimización,[137] traumatización y – a menudo en el caso de hombres, niños y mujeres de grupos marginados – encarcelamientos excesivos.[138]

Estas dinámicas se pueden agravar en el dominio informático. Los delitos a menudo son nuevos o están mal definidos,[139] lo que deja espacio para que los sesgos de género y supuestos esencialistas entren a las investigaciones y los procesamientos.[140] Cada vez es más común que los abusadores usen "stalkerware" para monitorear a las víctimas; no obstante, un estudio reciente de las leyes estadounidenses y canadienses reveló que los fabricantes y usuarios rara vez son enjuiciados por el uso de tecnología maliciosa.[141] El hacer cumplir las leyes sobre lo cibernético sigue siendo un campo primordialmente en manos de empleados masculinos, sufre de falta de jueces capacitados y está caracterizado por las normas del género masculino.[142] Es común en las investigaciones criminales, por ejemplo, confiscar los dispositivos de las víctimas como evidencia (lo cual podría plantear un riesgo de seguridad personal) y descargar todas las imágenes, lo

cual viola la privacidad de las víctimas y potencialmente socaba su credibilidad en casos de abuso o acoso sexual.[143] Si las víctimas no desean compartir sus datos personales, las autoridades en algunos casos se han negado a procesar el caso.[144] El uso creciente de la IA en las investigaciones de ciberseguridad y la justicia penal vuelve vulnerables a las víctimas, los infractores y a todo el sistema del orden público tanto a sesos de género como raciales, al amplificar los problemas y las desigualdades relacionados con el género.[145]

Los marcos legales actuales para las investigaciones de ciberincidentes, especialmente los que involucran a los servicios de inteligencia y las fuerzas del orden que acceden a datos u ordenan vigilancia electrónica utilizando software forense remoto, no toman en cuenta los impactos en cuanto al género de estas herramientas intrusivas. Vinculado a esto, los enfoques legales hacia los actores cibernéticos maliciosos pueden reflejar normas masculinistas para hacer cumplir la ley de manera general, particularmente aquellos que sugieren que las contrarrespuestas punitivas y agresivas son la mejor, y tal vez la única, opción de respuesta.[146]

El género es central para determinar qué es un acto malicioso, o sea, identificar un delito y determinar la respuesta apropiada. Aunque en algunos casos esto lleva hacia una legislación sobre género directamente, tal como la criminalización de ciertas formas de acoso en línea con respecto al género o sexualizada (por ejemplo, hackear para conseguir y publicar fotos sin consentimiento, a veces para "sextorsionar" contenido sexual

Transversalización de género

La transversalización de género "es el proceso de evaluar las implicaciones para niñas y niños y hombres y mujeres de cualquier acción planeada, incluyendo la legislación, las políticas y los programas".[154] Es la estrategia principal del Sistema de las Naciones Unidas para acelerar el progreso en la igualdad de género, al asegurarse que las perspectivas y necesidades diferenciadas de mujeres y niñas y de hombres y niños sean incorporadas en todos los procesos relacionados con políticas, para garantizar la inclusión y evitar la perpetuación de las inequidades.[155]

adicional),[147] una perspectiva de género es mucho más amplia. Conlleva, en otras palabras, un análisis sistemático de género de los problemas que a primera vista no parecieran ser "sobre" mujeres y niñas (u hombres y niños). Por ejemplo, las respuestas legales a las filtraciones de información privada o los hackeos de registros médicos deben considerar los impactos en cuanto al género de estos incidentes. Además de potencialmente exponer información médica privada de todos los involucrados,[148] las mujeres con capacidad de embarazarse podrían ser afectadas de manera particular por la publicación de su historial reproductivo,[149] mientras que las vidas, los medios de vida y el bienestar de las personas LGBTQ+ podrían ponerse en peligro al publicar e involuntariamente "sacar del clóset" sus identidades.[150]

Los marcos legales que responden a actos maliciosos en el ciberespacio con frecuencia se precipitan de una manera alarmista, en vez de fortalecedora. Esto produce control estatal y violaciones a la privacidad, perjuicios o revictimización de quienes están tratando de proteger.[151] Por ejemplo, las leyes que tienen la intención de proteger a las mujeres o a los grupos vulnerables de la violencia en línea pueden ser paternalistas, crear más posibilidades de control, dominio y violación de la privacidad relacionada con el género al ser implementadas.[152]

Todas estos cambios en las políticas requieren apoyo y acción de parte de los órganos legislativos nacionales como actores primordiales responsables de la redacción de la legislación sobre ciberseguridad (y la incorporación del género en estas).[153] Por lo tanto, es importante facilitar un proceso legislativo (y de vigilancia) abierto y participativo que involucre a todos los actores, especialmente a la sociedad civil, los grupos de derechos de las mujeres y las organizaciones de derechos de las personas LGBTQ+ en la discusión.

5.2 Áreas adicionales a investigar

Por una parte, necesitamos un mejor entendimiento de los vínculos entre las normas relacionadas con la conducta estatal responsable y, por la otra, las respuestas de la justicia penal nacional a las ciberamenazas y los actos maliciosos en el ciberespacio. Cada vez más los Estados recurren a la justicia penal para la atribución, la investigación y el procesamiento de actos cometidos por adversarios, conectando la ciberseguridad con las complejas dinámicas de género de las leyes nacionales y los sistemas de justicia penal nacionales. Aunque esto no significa que necesariamente deben unirse los

procesos de las Naciones Unidas sobre la ciberseguridad internacional y el cibercrimen, el vínculo entre ambos debería ser reconocido e investigado más a fondo para evitar caer en esfuerzos aislados para integrar el género en la ciberseguridad.

Las respuestas legales a los actos maliciosos en el ciberespacio ponen a nuestro enfoque hacia la ciberseguridad centrado en lo cibernético de nuevo en contacto con los enfoques centrados en el ser humano mediante las leyes sobre la violencia cibernética basada en género, el abuso doméstico y la legislación contra el acoso. El uso eficaz de las leyes para abordar la ciberseguridad, por ende, requiere tomar en cuenta los impactos sobre el género de todas las leyes que afrontan las ciberamenazas, desde las amenazas a la integridad, confidencialidad y disponibilidad de datos en los sistemas de cómputo hasta los perjuicios a los individuos.

Se requiere investigación adicional para evaluar si esta disparidad produce diferentes experiencias en cuanto al "soporte técnico" entre hombres, mujeres y personas no binarias. Este trabajo también debería investigar si la identidad de género en la comunidad técnica sobre ciberseguridad influye en la voluntad de las personas de reportar problemas de ciberseguridad percibidos como personales (por ejemplo, la pornovenganza, las estafas románticas, el robo de identidad).

5.3. Recomendaciones

- Los órganos legislativos nacionales, en consulta con una amplia gama de actores, incluyendo a la sociedad civil y la industria privada, deben identificar el impacto sobre el género de (a) los incidentes de ciberseguridad que se procuran atender mediante las leyes, (b) la ley misma y (c) su implementación.
- Los Estados, en consulta con múltiples actores, deben recopilar datos desagregados por género e igualdad para analizar el impacto de las respuestas legales existentes y revisarlas con base en los resultados.
- Los Estados, en cooperación con la sociedad civil y las empresas, deben crear e implementar una lista clara de indicadores para monitorear el impacto sobre el género de las respuestas legales a las amenazas contra la ciberseguridad.
- Los Estados, en consulta con otros actores, deben identificar los obstáculos relacionados con el género del acceso a la justicia (o sea, las fuerzas del orden y el sistema judicial) y deben trabajar para eliminar dichos obstáculos. Capacitar a la policía, fiscales y jueces es esencial.

- Las organizaciones internacionales y regionales, los Estados y los órganos legislativos deben promover el trabajo de promoción de parlamentos sensibles al género. Las preocupaciones de género deben ser un componente regular del comité legislativo que vigila las leyes y prácticas de ciberseguridad.
- La legislación sobre la igualdad de género y sexual (y los riesgos y la discriminación), tales como las leyes contra la violencia de pareja, deben incorporar la atención a las tecnologías digitales.[156] Esto debe complementarse con la identificación de los roles y las responsabilidades del sector privado en la implementación de marcos legales sensibles al género y los cambios en la estructura de la interacción digital.
- Las respuestas legales deben reconocer las limitaciones de la justicia penal. Aunque la responsabilidad criminal es una herramienta legal importante también, no debe ser la única solución, particularmente en casos cuando la creación de normas, la justicia restitutiva y las medidas alternativas serían más apropiadas o eficaces para abordar los perjuicios y evitar incidentes futuros.[157]

6. Conclusiones

Este informe adopta un enfoque de género hacia la ciberseguridad que propone un marco nuevo para ayudar a personas creadoras de políticas y profesionales a pensar con base en las implicaciones de género en el diseño, la defensa y la respuesta de la ciberseguridad. Este marco de tres pilares aborda la percepción errónea común de que los aspectos técnicos o tecnológicos de la ciberseguridad son neutros en cuanto al género y, por ende, ciegos al género.

Este análisis identifica áreas claves en que las prácticas de ciberseguridad requieren un análisis de género u otras intervenciones de políticas sobre género. El enfoque de tres pilares, aunque simplificado y esquemático, permite una delineación analítica clara de diferentes dinámicas de género. En la práctica, hay un traslape amplio e interacción entre los pilares, de modo que las mejoras en uno llevarían a mejoras en los demás.

El análisis sistemático se complementa con tres casos de estudio profundos que analizan las normas sobre ciberseguridad, el talento y la experticia y las respuestas legales. Estos casos de estudio exploran el alcance de la investigación existente y las políticas sobre estos tres temas y enfatizan la investigación que ya ha indicado la existencia de desigualdades de género u otros efectos nocivos y señala áreas que requieren investigación adicional e intervenciones en las políticas para contrarrestar dichos perjuicios. Cada uno de estos casos de estudio llevan a varias recomendaciones que pueden ser implementadas por los Estados junto con otros actores, incluyendo la academia, las organizaciones de la sociedad civil, instituciones internacionales y regionales y empresas.

También hacemos la recomendación general de la necesidad de generar e implementar capacitación sobre género y ciberseguridad en todas las organizaciones y sectores del campo. Este es un prerrequisito esencial para mejorar aún más la igualdad y equidad de género dentro del sector, además de desarrollar experticia sustantiva en el análisis de género como una destreza profesional.

El objetivo general de esta investigación es garantizar que la ciberseguridad mejore la seguridad de las personas de todas las identidades y expresiones de género, además de la

paz y seguridad internacionales. La conclusión fundamental es que estos dos niveles de seguridad no pueden estar separados.

Notas finales

1. No binario se usa aquí como un término amplio para referirnos a las identidades de género que no se alinean con la dualidad del género (o sea, hombres/masculinidad y mujeres/feminidad). Este incluye identidades agénero, de género fluido y genderqueer, así como también las muchas identidades de género no binario específicas a un contexto que existen en las sociedades alrededor del mundo. El término, por ende, debe entenderse de manera amplia, en vez de simplemente como una tercera opción monolítica singular. No binario no es sinónimo de trans, el cual generalmente se refiere a personas cuya identidad de género no concuerda cómodamente con el sexo que les fue asignado al nacer, pues muchas de estas personas se identifican como hombres o mujeres. Para más sobre este tema, vea United Nations Free & Equal, "Definitions", https://www.unfe.org/definitions/ y Stonewall, "Glossary of Terms", https://www.stonewall.org.uk/help-advice/faqs-and-glossary/glossary-terms#n.

2. Debido a las limitaciones de espacio y a una relativa falta de investigación existente, es informe analiza primordialmente las diferentes experiencias y oportunidades de hombres y mujeres predominantemente cisgénero en ciberseguridad. Sin embargo, un análisis robusto de género debería ser interseccional: atento a las maneras en que múltiples formas de poder social, relacionado con clase, raza, colonialidad, nacionalidad, habilidad, etnicidad, casta, orientación sexual, edad y expresión de género, etc. trabajan junto al género para producir patrones de marginalización y exclusión. Es esencial realizar investigación adicional sobre estas intersecciones tanto en el Norte Global como en el Sur Global. K. Crenshaw, "Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Colour", Stanford Law Review, vol. 43, no. 6, July 1991, pp. 1241–1299, https://doi.org/10.2307/1229039 y Combahee River Collective, "A Black Feminist Statement", Women's Studies Quarterly, vol. 42, no. 3/4, fall/winter 2014, pp. 271–280, https://www.jstor.org/stable/243650101977, pp. 210–218.

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

4. Por ejemplo, las declaraciones enviadas al GTCA por Estados y actores no estatales, las Naciones Unidas, United Nations, Office for Disarmament Affairs, "Open-ended Working Group", https://www.un.org/disarmament/open-ended-working-group/ e "Informal Intersessional Consultative Meeting of the Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security: Chair's Summary", 2–4 December 2019, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/200128-OEWG-Chairs-letter-on-the-summary-report-of-the-informal-intersessional-consultative-meeting-from-2-4-December-2019.pdf. I. Nakamitsu, Opening Address by to the Group of Governmental Experts on Advancing responsible State Behaviour in Cyberspace in the Context of International Security, 9 December 2019, https://www.un.org/disarmament/wp-content/uploads/2019/12/HR-addresses-GGE-on-advancing-responsible-State-behaviour-in-cyberspace-.pdf.

5. Para información detallada sobre las declaraciones nacionales que resaltan la importancia de la incorporación del género en el proceso del GTCA, vea Cyber Peace & Security Monitor, vol. 1 no. 7, 18 February 2020, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.7.pdf. Vea también "Canada's Proposal for the Report of the 2019–20 United Nations Open-Ended Working Group on 'Developments in the Field of Information and Telecommunications in the Context of International Security'", Working paper submitted by Canada, https://www.un.org/disarmament/wp-content/uploads/2019/09/canadian-position-paper-oewg-en.pdf.

6. Sobre la distinción entre identidad de género y expresión de género, vea Ontario Human Rights Commission (OHRC), Policy on Preventing Discrimination Because of Gender Identity and Gender Expression, 14 April 2014, Appendix B, "Glossary for Understanding Gender Identity and Expression", http://www.ohrc.on.ca/en/policy-preventing-discrimination-because-gender-identity-and-gender-expression/appendix-b-glossary-understanding-gender-identity-and-expression.

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

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

9. Por ejemplo, Verizon atribuye el 71% de los incidentes a delitos por motivaciones económicas y solo un 25% a espionaje, Verizon Data Breach Investigations Report 2019, 2019, https://enterprise.verizon.com/en-nl/resources/reports/dbir/2019/summary-of-findings/

10. Por ejemplo, mediante la generación automática de malware o el control de botnets.

11. J. Shires, "Between Multistakeholderism and Sovereignty: Cyber Norms in Egypt and the Gulf States", War on the Rocks, 12 October 2018. https://perma.cc/L4CL-2B8A. Vea también P. Cornish, "Governing Cyberspace through Constructive Ambiguity", Survival, vol. 57, no. 3, May 2015, pp. 153–76, https://doi.org/10.1080/00396338.2015.1046230; M. Raymond and L. DeNardis, "Multistakeholderism: Anatomy of an Inchoate Global Institution", International Theory, vol. 7, no. 3, November 2015, pp. 572–616, https://doi.org/10.1017/S1752971915000081 y A. Grigsby, "The End of Cyber Norms", Survival, vol. 59, no. 6, November 2017, pp. 109–122, https://doi.org/10.1080/00396338.2017.1399730.

12. Vea, por ejemplo, National Coordinator for Security and Counterterrorism, "Cyber Security Assessment Netherlands", Ministry of Justice and Security, 2019, https://english.ncsc.nl/topics/cybersecurity-assessment-netherlands. El Comité sobre las Fuerzas Armadas del Senado de Estados Unidos celebró una reunión del subcomité de ciberseguridad sobre las fugas de información en abril del 2017, que llevó a descripciones de las fugas de información rusas como un problema de ciberseguridad en muchas publicaciones subsiguientes. Los estados "afines" siempre han incluido algunos controles de contenido en su legislación sobre terrorismo, pero la definición de terrorismo es otro tema delicado. Otra manera de plantear este punto es que nuestra definición de ciberseguridad usa una versión más limitada de la integridad de la triada tradicional de "Confidencialidad, Integridad, Disponibilidad" (CIA, sigla en inglés) en la seguridad informática.

13. Las operaciones de hackeo y fuga implican la obtención de datos sensibles mediante una ciberintrusión (hackeo) y la distribución de dichos datos en el dominio público (fuga). J. Shires, "Hack-and-Leak Operations: Intrusion and Influence in the Gulf", Journal of Cyber Policy, vol. 4, no. 2, 2019, pp. 235–56, https://doi.org/10.1080/23738871.2019.1636108 y J. Shires, "The Simulation of Scandal: Hack-and-Leak Operations, the Gulf States, and U.S. Politics", Texas National Security Review, vol. 3, no. 4, fall 2020, https://tnsr.org/2020/08/the-simulation-of-scandal-hack-and-leak-operations-the-gulf-states-and-u-s-politics/.

14. Vea el capítulo 5 de este informe.

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

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

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

18. Estos impactos incluyen a las mujeres en la vida política pública, la ciberintimidación de niños y niñas y personas jóvenes. K. Blake, M. Godwin and S. Whyte, "'I Sexually Identify as an Attack Helicopter': Incels, Trolls, and Non-Binary Gender Politics Online", First Monday, vol. 25, no. 9, 2020, https://doi.org/10.5210/fm.v25i9.10601; K.

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

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

20. El principal enfoque alternativo de este marco "centrado en lo cibernético" es lo que podría denominarse un enfoque "centrado en el ser humano", el cual es más común en los análisis de género. Para un ejemplo de dicho enfoque, consulte el trabajo que resalta el impacto diferenciado de ciertos tipos de ciberincidentes de acuerdo con el género (tal como, las desconexiones de la Internet, las infiltraciones de datos, etc.) en D. Brown and A. Pytlak, Why Gender Matters in International Cyber Security, Women's International League for Peace and Freedom (WILPF) and the Association for Progressive Communications (APC), April 2020, https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf. Al resaltar la experticia de esta manera, no queremos decir que otras formas (tales como la experticia sobre políticas) no son relevantes para la ciberseguridad; por el contrario, examinamos sus supuestos basados en género en los siguientes capítulos de este informe.

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

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

23. La "cadena de exterminio" es un modelo para representar los muchos pasos involucrados en un ciberataque (y, por lo tanto, las muchas oportunidades para que la defense de la ciberseguridad interrumpa el ataque). E.M. Hutchins, M.J. Cloppert and R.M. Amin, "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains", Lockheed Martin Corporation, 2010, https://lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

24. Propuestas por el cuarto Grupo de Expertos Gubernamentales (GEG) de las Naciones Unidas sobre los Avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional, General Assembly, A/70/174, 22 July 2015, http://undocs.org/A/70/174.

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

26. Estas extensos corpus de investigación se combinan con un enfoque designado "computación centrada en el ser humano", directamente más relevante para la ciberseguridad.

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

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

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

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

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

32. Vea por ejemplo los recursos en Refuge, "Tech abuse and tech safety resources", https://www.refuge.org.uk/our-work/forms-of-violence-and-abuse/tech-abuse-2/resources/.

33. Los modelos de amenazas basados en género también deberían estar presentes a nivel estatal, tal como en los procesos de acciones de vulnerabilidad. Vea S. Herpig and A. Schwartz, "The Future of Vulnerabilities Equities Processes Around the World", Lawfare, 4 January 2019, https://perma.cc/6U3P-38JA.

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

35. E.g. A. Malik, K. Hiekkanen and M. Nieminen, "Privacy and Trust in Facebook Photo Sharing: Age and Gender Differences", Program, vol. 50, no. 4 (January 2016), pp. 462–480, https://doi.org/10.1108/PROG-02-2016-0012 y and S. Tifferet, "Gender Differences in Privacy Tendencies on Social Network Sites: A Meta-Analysis", Computers in Human Behavior, vol. 93, April 2019, pp. 1–12, https://doi.org/10.1016/j.chb.2018.11.046. Para una conclusión contraria más antigua, vea d. boyd and E. Hargittai, "View of Facebook Privacy Settings: Who Cares?", First Monday, vol. 15, no. 8, 2010, https://doi.org/10.5210/fm.v15i8.3086.

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

37. Ibid.

38. Debe tomarse en cuenta que los derechos de los y las menores de edad a la privacidad, la expresión y la seguridad (y las maneras en que estos podrían estar en conflicto con los deseos de los padres de familia) a menudo no figuran – aunque debieran – de manera predominante en las discusiones sobre ciberética, ciberseguridad y cibergobernanza. Para una revisión general de esta complejidades, vea S. Livingstone and B. O'Neill, "Children's Rights Online: Challenges, Dilemmas and Emerging Directions", In S. van der Hof, B. van den Berg and B. Schermer (eds.), Minding Minors Wandering the Web: Regulating Online Child Safety, TMC Asser Press, 2014, pp. 19–38, https://doi.org/10.1007/978-94-6265-005-3_2.

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

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

41. ISO/IEC Directives, Part 2, "Principles and Rules for the Structure and Drafting of ISO and IEC Documents", 8th edn., 2018, https://www.iso.org/sites/directives/current/part2/index.xhtml#_idTextAnchor007, Section 3.1.2. La

definición de la ISO agrega que una norma tiene que ser "establecida por consenso y aprobada por un órgano reconocido". Vea también la definición de la Organización Mundial del Comercio (OMC: "las normas establecen las características específicas de un producto – tal como su tamaño, forma, diseño, funciones y desempeño, o la manera en que está etiquetado o empacado", además del proceso específico y los métodos de producción de dicho producto. World Trade Organization, "Technical Information on Technical Barriers to Trade", https://www.wto.org/english/tratop_e/tbt_e/tbt_info_e.htm.

42. Los reglamentos pueden hacer referencia a las normas, pero los órganos de normas nacionales generalmente están separados de los reguladores (pues es una buena práctica de la OMC). Ibid.

43. Enlace hacia el mapa de ruta completo de las normas de ciberseguridad y las organizaciones que las están elaborando: International Telecommunication Union (ITU), "Security Standards Under Development", ICT Security Standards Roadmap, https://www.itu.int/en/ITU-T/studygroups/com17/ict/Pages/ict-part03.aspx.

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

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

46. El requerimiento de que el desarrollo de capacidades en ciberseguridad sea sensible al género, inclusivo y no discriminatorio se alinea con los compromisos generales de las Naciones Unidas y sus Estados Miembro con la equidad de género. Estos se expresan formalmente en la Convención sobre la eliminación de todas las formas de discriminación contra la mujer y se reflejan en los Objetivos del Milenio y los Objetivos de Desarrollo Sostenibles (particularmente en el ODS 5). UNICEF Regional Office for South Asia, Gender Equality: Glossary of Terms and Concepts, November 2017, https://www.unicef.org/rosa/media/1761/file/Gender%20glossary%20of%20terms%20and%20concepts%20.pdf.

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

48. United Nations Economic Commission for Europe, "Gender Responsive Standards", 2019, https://www.unece.org/fileadmin/DAM/trade/Publications/ECE_TRADE_445E.pdf, pp. 8–9. Para una amplia gama de ejemplos, vea también C.C. Perez, Invisible Women: Data Bias in a World Designed for Men, Harry N. Abrams, 2019.

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

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

51. Existen normas similares para ciertos sectores, por ejemplo, las DSS de PCI por lo general se consideran el equivalente de las ISO 27001 para el sector financiero.

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

53. Consideramos tanto el Plan de Acción sobre Género aplicado en toda las normas ISO y el trabajo del comité que gestiona la serie 27000 (ISO/IEC JTC1/SC 27) pues son dos iniciativas separadas.

54. Esta es una decisión muy reciente. Los entrevistados sugirieron que el formato exacto de estos datos y su distribución, cuando se recopilen, aún no se han decidido.

55. Agradecemos a Christina Runnegar por este punto.

56. La implicación es dual: primero, que la actividad descrita usando este término se ve como menos importante

debido a su estatus inferior y, segundo, que la actividad se asigna con base en el género, transfiriendo este estatus inferior a aquellos que realizan el trabajo. Para múltiples ejemplos de este proceso en acción, vea M. Hicks, M., Programmed Inequality: How Britain Discarded Women Technologists and Lost Its Edge in Computing, MIT Press, 2017.

57. Información obtenida durante las entrevistas con los interesados. Los autores desean agradecer a Noelia García Nebra y al Dr. Edward Humphreys por su generosa ayuda con la recopilación de información relevante y por sus útiles ideas sobre los esfuerzos realizados por la ISO con relación al género. Para una discusión del lenguaje sesgado en cuanto al género que enmarca el "sentido común" de la ciberseguridad, vea A. Lee, "It Starts with Words: Unconscious Bias in Gender, Race, and Class in Tech Terminology", 19 August 2020, https://www.localizationlab.org/blog/2020/8/19/it-starts-with-words-unconscious-bias-in-gender-race-and-class-in-tech-terminology.

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

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

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

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

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

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

64. Vea el proyecto de investigación: F. J. Egloff and J. Shires, "Political Violence in Cyberspace", ETH Zürich, https://css.ethz.ch/en/research/research-projects/political-violence-in-cyberspace.html.

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

66. LGBTQ+ se refiere específicamente a lesbianas, gais, bisexuales, personas transgénero y queer, pero el signo + significa su inclusión de personas de diversas, y a menudo marginalizadas, identidades de género, expresiones de género y orientaciones sexuales (que no son sinónimo).

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

68. El monitoreo de las amenazas puede variar en escala desde el fraude hasta el robo de identidad de individuos hasta el ciberespionaje corporativo a gran escala.

69. D. Brown and A. Pytlak, Why Gender Matters in International Cyber Security, Women's International League for

Peace and Freedom (WILPF) and the Association for Progressive Communications (APC), April 2020, https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf.

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

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

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

73. Esto se da especialmente en el caso de los llamados ataques "whaling" cuyo blanco son los individuos en puestos ejecutivos o de poder.

74. J. Shires, "Cyber-Noir: Cybersecurity and Popular Culture", Contemporary Security Policy, vol. 41, no. 1, 2020, pp. 82–107, https://doi.org/10.1080/13523260.2019.1670006. Para ejemplos del sexismo nocivo de las tecnologías en la división de ciberoperaciones de ofensiva de la Agencia Nacional de Seguridad (NSA, sigla en inglés), vea también B. Gellman, Dark Mirror, 2020, pp. 203–204.

75. Nótese que los seguros de ciberseguridad se ofrecen de manera privada pero, como con todo seguro, están sujetos a regulaciones estatales, un punto de entrada para la creación de políticas. La investigación reciente indica que, debido a la dinámica del mercado, los seguros de ciberseguridad actualmente son una forma débil de gobernanza no estatal que no promueve estándares mínimos y el uso de auditorías regulares de las capacidades informáticas. Consulta a Daniel Woods, Security and Privacy Lab, University of Innsbruck y D.W. Woods and T. Moore, "Does Insurance Have a Future in Governing Cybersecurity?", IEEE Security & Privacy, vol. 18, no. 1, 2019, pp. 21–27, https://doi.org/10.1109/MSEC.2019.2935702.

76. Para un repaso general de los intentos de incorporar el género en los seguros, vea K. Miles, M. Wiedmaier-Pfister and M.-C. Dankmeyer, Mainstreaming Gender and Targeting Women in Inclusive Insurance: Perspectives and Emerging Lessons, Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), 2017, https://www.ifc.org/wps/wcm/connect/topics_ext_content/ifc_external_corporate_site/gender+at+ifc/resources/women-in-inclusive-insurance. Para un ejemplo de la complejidad de las regulaciones de los seguros y la equidad de género, vea la discusión de la Directiva sobre Género de la UE sobre los seguros para automóviles. P. Collinson, "How an EU Gender Equality Ruling Widened Inequality", The Guardian, 14 January 2017, https://www.theguardian.com/money/blog/2017/jan/14/eu-gender-ruling-car-insurance-inequality-worse y European Commission, "EU Rules on Gender-Neutral Pricing in Insurance Industry Enter into Force", Press release, 20 December 2012, https://ec.europa.eu/commission/presscorner/detail/en/IP_12_1430.

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

78. Vea los informes en la página web del Global Forum on Cyber Expertise (GFCE), https://thegfce.org/impact/. En el contexto británico, para conocer sobre un ejemplo de las mejores prácticas en esta área, vea National Cyber Security Centre and KPMG, Decrypting Diversity: Diversity and Inclusion in Cyber Security, 2020, https://www.ncsc.gov.uk/report/diversity-and-inclusion-in-cyber-security-report.

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

80. Los roles de los profesionales en ciberseguridad varían muchísimo desde puestos de diseño técnico, hackeo y codificación, pasando por ventas, mercadeo y recursos humanos, hasta diplomacia, regulación, cumplimiento de las leyes y defensoría. Vea Help Net Security, "Women are Increasingly Climbing the Cybersecurity Leadership Ladder", 3 April 2019, https://www.helpnetsecurity.com/2019/04/03/women-cybersecurity-workforce/ y S.

Morgan, "Women Represent 20 Percent of The Global Cybersecurity Workforce in 2019", Cybercrime Magazine, 28 March 2019, https://cybersecurityventures.com/women-in-cybersecurity/.

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

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

83. Vea, por ejemplo, (con nuestro agradecimiento a Beatrice Martini), Out in Science, Engineering, and Technology, https://ostem.org; Lesbians Who Tech, https://lesbianswhotech.org/debug2020/; Trans Tech, https://transtechsocial.org; Outreachy, https://outreachy.org y Diana Initiative, https://dianainitiative.org.

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

85. No obstante, es importante que tales iniciativas a menudo no son interseccionales. A pesar de que muchas mujeres de color del Sur Global trabajan en ciberseguridad, tales eventos con frecuencia aumentan la visibilidad de mujeres blancas principalmente del Norte Global.

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

87. D.T. Ireland et al., "(Un)Hidden Figures: A Synthesis of Research Examining the Intersectional Experiences of Black Women and Girls in STEM Education", Review of Research in Education, vol. 42, no. 1, 2018, pp. 226–254; A. Sey and N. Hafkin (eds.), Taking Stock: Data and Evidence on Gender Digital Equality, United Nations University, March 2019, https://i.unu.edu/media/cs.unu.edu/attachment/4040/EQUALS-Research-Report-2019.pdf; UN News, "'The World Needs Science and Science Needs Women', UN Says on International Day", 11 February 2017, https://news.un.org/en/story/2017/02/551212-world-needs-science-and-science-needs-women-un-says-international-day; UNESCO Science Report, Towards 2030: Executive Summary, 2015, UNESCO, https://unesdoc.unesco.org/ark:/48223/pf0000235407; S. Cheryan et al., "Ambient Belonging: How Stereotypical Cues Impact Gender Participation in Computer Science", Journal of Personality and Social Psychology, vol. 97, no. 6, 2009, pp. 1045–1060, http://doi.org/10.1037/a0016239 y UNESCO Institute for Statistics (UIS), "Women in Science", Fact Sheet no. 55, June 2015, http://uis.unesco.org/sites/default/files/documents/fs55-women-in-science-2019-en.pdf

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

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

90. F.J. García-Peñalvo, "Innovative Teaching Approaches to Attract, Engage, and Maintain Women in STEM: W-

STEM Project", 2019, http://doi.org/10.5281/zenodo.3538939.

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

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

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

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

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

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

97. Ibid, p. 5.

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

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

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

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

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

103. Frost & Sullivan, 2017 Global Information Security Workforce Study: Benchmarking Workforce Capacity and Response to Cyber Risk, International Information System Security Certification Consortium, 2017, https://www.isc2.org/-/media/Files/Research/ISC2-Women-in-Cybersecurity-2017.ashx.

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

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

106. Por ejemplo, W.R. Poster, "Cybersecurity Needs Women", Nature, 26 March 2018, https://www.nature.com/articles/d41586-018-03327-w. Existe alguna evidencia de que esto podría estar cambiando. P. Roberts, "Forget 'Brogrammers', Women Have the Edge in DEFCON Social Engineering Contest", Threat Post, 21 May 2012, https://threatpost.com/forget-brogrammers-women-have-edge-defcon-social-engineering-contest-052112/76587/.

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

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

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

110. Vea varias redes de mujeres en ciberseguridad, incluyendo el Foro de Género del GFCE, Mujeres Holandesas en Ciberseguridad (WiCS), Mujeres en Ciberseguridad (WiCyS), Sociedad de Mujeres en Ciberseguridad y Foro Ciber de Mujeres. Vea también National Cyber Security Centre and KPMG, Decrypting Diversity: Diversity and Inclusion in Cyber Security, 2020, https://www.ncsc.gov.uk/report/diversity-and-inclusion-in-cyber-security-report.

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

112. Consulta a Julia Slupska, University of Oxford.

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

114. Para una ilustración de los roles y las destrezas asociadas con hombres y mujeres en la ciberseguridad en Estados Unidos, vea C. Martinez, "Cybersecurity: Why You Should Care About the Skills and Gender Gap", Steppingblocks,
https://blog.steppingblocks.com/cyber-security-gender-and-skills-gap

115. La consulta a expertos sugiere que las mujeres en los Balcanes y la antigua Unión Soviética, por ejemplo, podrían estar mejora representadas en puestos informáticos estatales que en el sector privado. Sería útil saber si esto es cierto (y, si es así, por qué), si esto se traduce en su participación significativa y si podría ofrecer lecciones valiosas para otros contextos.

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

117. Por ejemplo, vea datos para Estados Unidos en "Percentage of Employed Women in Computing-Related Occupations in the United States from 2000 to 2019", https://www.statista.com/statistics/311972/us-women-computer-workers/ y para la UE, Eurostat, "ICT Specialists in Employment", October 2019, https://ec.europa.eu/eurostat/statistics-xplained/index.php/ICT_specialists_in_employment#ICT_specialists_by_sex.

118. L.M. Tanczer, I. Brass and M. Carr, "CSIRTs and Global Cybersecurity: How Technical Experts Support Science Diplomacy", Global Policy, vol. 9, no. S3, November 2018, pp. 60–66, https://doi.org/10.1111/1758-5899.12625. Vea concretamente las observaciones de que los CSIRT promueven una "cultura global de expertos y realizan importantes procesos de construcción de comunidades" (p. 62) y que incorporan "diferencias culturales . . . delicadas" (p. 63).

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

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

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

122. Consulta a Daniel Woods, Security and Privacy Lab, University of Innsbruck.

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

124. Por ejemplo, la Directiva de Redes y Seguridad de la Información de la Unión Europea ordena a sus Estados miembro tener capacidades de ciberseguridad nacionales relacionadas con la preparación, tal como contar con un CERT nacional y realizar ejercicios cibernéticos.

125. Informe del Grupo de Expertos Gubernamentales de las Naciones Unidas sobre los avances en el campo de la información y las telecomunicaciones en el contexto de la seguridad internacional, General Assembly, A/70/174, 22 July 2015, http://undocs.org/A/70/174, paragraph 17(e).

126. Ibid, paragraph 13(h).

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

128. Esto podría atribuirse parcialmente a la falta de posiciones unificadas sobre cómo el derecho internacional se aplica en la realidad a las ciberoperaciones. Para un análisis de las posiciones de los Estados sobre la aplicación del derecho internacional, vea R. Przemysław, Application of International Law to Cyber Operations: A Comparative Analysis of States' Views, The Hague Program for Cyber Norms, March 2020, https://www.thehaguecybernorms.nl/research-and-publication-posts/application-of-international-law-to-cyber-operations-a-comparative-analysis-of-states-views.

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

130. Por ejemplo, en el 2020, Alemania presentó cargos contra un hackeador ruso quien supuestamente es empleado del Departamento Central de Inteligencia Rusa (GRU) por un ataque en el 2015 contra el Parlamento alemán. Vea C. Cimpanu, "German Authorities Charge Russian Hacker for 2015 Bundestag Hack", 5 May 2020, https://www.zdnet.com/article/german-authorities-charge-russian-hacker-for-2015-bundestag-hack/.

131. D. Shoker, "Making Gender Visible in Digital ICTs and International Security", Report submitted to Global Affairs Canada, 2019, https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf y D. Brown and A. Pytlak, Why Gender Matters in International Cyber Security, Women's International League for Peace and Freedom (WILPF) and the Association for Progressive Communications (APC), April 2020, https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf. .

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

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

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

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

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

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

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

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

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

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

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

143. Consulta al Equipo SafetyNet de la Red Nacional Estadounidense para Poner Fin a la Violencia Doméstica.

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

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

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

147. Por ejemplo el incidente de hackeo de Apple iCloud en el 2014 que produjo la publicación sin consentimiento de fotografías de desnudos de personas famosas. E. Grinberg and N. Chavez, "Connecticut Man Sentenced in Celebrity Photo Hacking Scandal", CNN, 30 August 2018, https://edition.cnn.com/2018/08/29/entertainment/celebrity-photo-hacking-sentence/index.html. Sobre la sextorsión, vea B. Wittes et al., "Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault", Brooking Institution, 11 May 2016, https://www.brookings.edu/research/sextortion-cybersecurity-teenagers-and-remote-sexual-assault/.

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

149. Privacy International, "Why Does Reproductive Health Surveillance in India Need Our Urgent Attention?", 24 February 2020, https://privacyinternational.org/long-read/3368/why-does-reproductive-health-surveillance-india-need-our-urgent-attention y J. Davis, "300,000 Records Breached in Ransomware Attack on Pennsylvania Health System", Healthcare IT News, 26 July 2017, https://www.healthcareitnews.com/news/300000-records-breached-ransomware-attack-pennsylvania-health-system.

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

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

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

153. Por ejemplo, iniciativas como la de la Inter-Parliamentary Union, Gender-Sensitive Parliaments: Executive Summary, 2011, http://archive.ipu.org/pdf/publications/gsp11ex-e.pdf.

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

155. European Institute for Gender Equality, "Gender Analysis", https://eige.europa.eu/gender-mainstreaming/methods-tools/gender-analysis. Vea además la herramienta GBA+ y el proceso de capacitación preparado por el gobierno canadiense, Status of Women Canada, "What is GBA+", 28 October 2020, https://cfc-swc.gc.ca/gba-acs/index-en.html.

156. Por ejemplo, L.M. Tanczer, "The Government Published Its Draft Domestic Abuse Bill, But Risks Ignoring the Growing Threat of Tech Abuse", 25 February 2019, Medium, https://medium.com/policy-postings/the-government-published-its-draft-domestic-abuse-bill-but-risks-ignoring-the-growing-threat-of-368a6fb70a14.
Para preparar y revisar las respuestas legales a los incidentes de ciberseguridad, los órganos legislativos nacionales pueden emplear las herramientas existentes tales como las guías preparadas por la OSCE o la Inter-Parliamentary Union sobre procesos legislativos sensibles al género. Vea OSCE Office for Democratic Institutions and Human Rights, Making Laws Work for Women and Men: A Practical Guide to Gender-Sensitive Legislation, 2017, https://www.legislationline.org/download/id/7545/file/Guidelines_Practical_guide_gender_sensitive_legislation_en.pdf.

157. Esto es particularmente cierto en el caso de hombres jóvenes (y un número más pequeños de mujeres jóvenes) que entran al cibercrimen, el hackeo y vandalismo antes de ser adultos. R. Marcinauskaitė, I. Pukanasytė and J. Šukytė, "Cyber Security Issues: Problematic Aspects of Hacking", Journal of Security and Sustainability Issues, vol. 8, no. 3, March 2019, http://doi.org/10.9770/jssi.2019.8.3(4).

Enfoques de género en la ciberseguridad: diseño, defensa y respuesta

Enfoques de género a la ciberseguridad explora cómo las normas de género dan forma a actividades específicas correspondientes al diseño, la defensa y la respuesta de la ciberseguridad. En cada uno de estos tres pilares, la investigación identifica dimensiones distintas de actividades relacionadas con la informática que tienen implicaciones en cuanto al género y, por ende, deben ser consideradas desde una perspectiva de género.

El informe propone recomendaciones para incorporar las consideraciones de género mediante políticas y prácticas internacionales de ciberseguridad, de modo que se garantice que la ciberseguridad mejore la seguridad de las personas de todas las identidades y expresiones de género, además de la paz y seguridad internacionales. La conclusión fundamental es que estos dos niveles de seguridad no pueden estar separados.