Actualización del Sistema: Hacia una agenda sobre Mujeres, Paz y Ciberseguridad

LISA SHARLAND | NETTA GOUSSAC | EMILIA CURREY |
GENEVIEVE FEELY | SARAH O'CONNOR

UNIDIR UNITED NATIONS INSTITUTE FOR DISARMAMENT RESEARCH

www.unidir.org

ACTUALIZACIÓN DEL SISTEMA: HACIA UNA AGENDA SOBRE MUJERES, PAZ Y CIBERSEGURIDAD

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 Canadá, Irlanda, Noruega, Reino Unido y Suecia.

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

Además, las autoras agradecen a Danielle Cave, Renata H. Dalaqua, Bart Hogeveen, Allison Pytlak, Tom Uren y Kerstin Vignard por sus valiosas observaciones y sugerencias, y el apoyo del Australian Strategic Policy Institute y su personal. Las autoras también desean reconocer a Shimona Mohan por su asistencia en la preparación de esta publicación.

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. 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

Sharland, Lisa et. al. 2021. *Actualización del Sistema: Hacia una Agenda sobre Mujeres, Paz y Ciberseguridad.* 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 patrocinadores 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 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 autoras

Lisa Sharland es investigadora principal y directora del programa Protecting Civilians and Human Security del Stimson Center en Washington DC. Anteriormente Lisa fue subdirectora de Seguridad Nacional, Estrategia y Defensa y Jefa del Programa Internacional del Australian Strategic Policy Institute, donde continúa colaborando como investigadora principal no residente. Ha trabajado en temas de seguridad multilateral por más de una década como consultora e investigadora sobre las mujeres, la paz y la seguridad, la seguridad internacional y la construcción de la paz.

Lisa trabajó anteriormente como asesora en políticas de defensa en la Misión Permanente de Australia ante las Naciones Unidas en Nueva York, donde brindaba asesoría sobre temas de políticas relacionadas con defensa y construcción de la paz y representaba a Australia en las negociaciones multilaterales en el Consejo de Seguridad y la Asamblea General.

Netta Goussac es investigadora senior asociada en la firma Lexbridge Lawyers. Ha trabajado como abogada internacional por más de una década en entidades como el Comité Internacional de la Cruz Roja y la Oficina de Derecho Internacional del Gobierno de Australia. Netta se especializa en marcos legales relacionados con el desarrollo, la adquisición y la transferencia de armas. Ha brindado asesoría legal y política con relación a las nuevas tecnología de guerra, incluyendo armas autónomas, aplicaciones militares de inteligencia artificial, ciberseguridad y seguridad en el espacio.

Desde el 2017, Netta ha participado en el Grupo de Personas Expertas Gubernamentales sobre sistemas de armas autónomas letales. Del 2010 al 2013, participó en la negociación del Tratado sobre el Comercio de Armas, 2013, y posteriormente trabajó para promover la adhesión universal a sus normas. Uno de los enfoques del trabajo de Netta es apoyar

la implementación del derecho internacional mediante la legislación nacional, las políticas, la doctrina y la capacitación. Ha brindado servicios técnicos, de consultoría y desarrollo de capacidades en el Pacífico, Asia y Europa.

Emilia Currey fue investigadora del International Cyber Policy Centre del Australian Strategic Policy Institute. Emilia tiene una Licenciatura en Derecho (Hons.) de la Australian National University. Sus intereses en la investigación incluyen temas sobre derecho internacional humanitario, interferencia extranjera, género y derechos humanos.

Genevieve Feely es abogada de la Suprema Corte de Queensland. Fue investigadora del Programa Internacional del Australian Strategic Policy Institute. Sus intereses actuales en investigación incluyen las Naciones Unidas, el multilateralismo, la construcción de la paz y la agenda sobre Mujeres, Paz y Seguridad. Antes de trabajar en el Australian Strategic Policy Institute, laboró en la Cuarta Comisión en la Misión Permanente de Australia ante las Naciones Unidas en Nueva York, donde estuvo a cargo de una variedad de temas sobre paz y seguridad, incluyendo la construcción de la paz y descolonización.

Sarah O'Connor fue investigadora en el International Cyber Policy Centre del Australian Strategic Policy Institute. Más recientemente, Sarah trabajó como investigadora adjunta en el Tech Policy Design Centre de la Australian National University. Sarah tiene una Licenciatura en Relaciones Internacionales (Hons.), una Maestría en Derecho Internacional (LLM) y una Maestría en Cibernética Aplicada (MAppCyb) de la Australian National University. Sus intereses en investigación incluyen derecho internacional, ciberseguridad y seguridad en el espacio, además de el diseño, el desarrollo, la instalación y el retiro de nuevas tecnologías emergentes e imaginadas.

Tabla de Contenido

Lista de siglas y abreviaturas

GEG	Grupos de Personas Expertas Gubernamentales
GTCA	Grupo de Trabajo de Composición Abierta
IA	Inteligencia artificial
ISIS	Estado Islámico en Iraq y el Levante
MPS	Mujeres, Paz y Seguridad
PAN	Plan de Acción Nacional
PAR	Plan de Acción Regional
TIC	Tecnologías de la Información y la Comunicación

Resumen ejecutivo

Conforme la agenda Mujeres, Paz y Seguridad (MPS) entra en su tercera década es crucial asegurarnos de que sea apta para abordar los asuntos de seguridad nuevos y emergentes, tales como las ciberamenazas y sus implicaciones con relación al género. Hacer esto requiere un cambio de enfoque para ir más allá del conflicto tradicional con el fin de abordar otros contextos donde ocurre violencia contra las mujeres, incluyendo el ciberespacio.

La accesibilidad y naturaleza inatribuible del ciberespacio han expuesto a las mujeres a cantidades desproporcionadas de acoso y hostigamiento en línea, además de campañas focalizadas de desinformación para disuadirlas de participar en política. Esto se ha vuelto más acuciante a la luz de la pandemia del COVID 19, conforme el mundo daba un giro hacia lo digital y notaba un aumento en la violencia en línea, la misoginia y los discursos de odio dirigidos hacia las mujeres.

La relación entre las amenazas con asistencia de la informática y la ciberseguridad no se ha explorado exhaustivamente como parte del desarrollo de la agenda normativa sobre MPS. Potenciar la ciberseguridad usando la agenda MPS puede promover un ciberespacio inclusivo en cuanto al género que proteja los derechos de las mujeres y niñas y que incorpore las lecciones aprendidas de los procesos tradicionales de paz y seguridad para el beneficio de un mundo digital sostenible, abierto, libre y estable. Asimismo, un examen del ciberespacio a través del lente de la agenda MPS demuestra que estos incidentes inherentemente están vinculados a la paz y la seguridad internacionales.

Este trabajo presenta un análisis más detallado de los temas cibernéticos que afectan las metas de la agenda MPS. Identifica seis áreas prioritarias que deben ser abordadas para reducir la brecha entre MPS y la ciberseguridad, a saber:

- la participación de las mujeres en las negociaciones de ciberseguridad;
- la ciberviolencia contra las mujeres y niñas;
- el acoso en línea y la participación de las mujeres en los procesos políticos;
- el género y la radicalización en línea;
- los impactos de los ciberincidentes en cuanto al género y
- los sesgos de género en las tecnologías digitales.

Traer estas consideraciones al primer plano de la agenda MPS producirá una muy necesaria 'actualización del sistema' y asegurará que la comunidad internacional esté equipada para lidiar con los desafíos de seguridad internacional del siglo veintiuno y sus implicaciones en cuanto al género.

Recomendaciones principales

Para enfrentar estos desafíos, este estudio recomienda un enfoque integrado que simultáneamente potencie la agenda MPS e iniciativas relacionadas con la ciberseguridad internacional.

Establecer la agenda a nivel internacional

- Fomentar iniciativas para aumentar la participación significativa de las mujeres en las negociaciones de ciberseguridad y entender las barreras para su participación en procesos multilaterales y multiparticipativos.
- Integrar las consideraciones de género en las declaraciones nacionales y propuestas de lenguaje como parte de un proceso participativo de las Naciones Unidas y las múltiples partes interesadas que se enfocan en la ciberseguridad internacional y las tecnologías digitales.
- Establecer la 'ciberseguridad' como un tema en el próximo debate bajo el punto en la agenda sobre 'mujeres y paz y seguridad' en el Consejo de Seguridad.
- Abordar sistemáticamente la ciberseguridad, incluyendo los aspectos e impactos del género de los ciberincidentes, en el informe anual de la Secretaría General sobre MPS.
- Garantizar que los diálogos multiparticipativos entre los Estados, la sociedad civil y las empresas de plataformas tecnológicas y redes sociales consideren las dinámicas de género cuando proponen soluciones para restringir la diseminación de contenido

terrorista y la desinformación en línea.

Desarrollo de políticas a nivel nacional

- Garantizar que las políticas y actividades nacionales de ciberseguridad de los gobiernos incorporen a todos los niveles diversas perspectivas de género como parte de su desarrollo e implementación.
- Preparar y/o fortalecer leyes, políticas y prácticas de ciberseguridad inclusivas en cuanto al género que respeten los derechos de las mujeres y niñas y que sean capaces de identificar y responder a sus necesidades en cuanto a la ciberseguridad.
- Proteger el espacio digital para la participación cívica de las mujeres y niñas, además de prevenir la ciberviolencia contra ellas.
- Aumentar la conciencia sobre qué es el ciberabuso preparando campañas públicas sobre este tema.
- Adoptar leyes que criminalicen el ciberhostigamiento y el ciberacoso y atender otras necesidades institucionales, como los mecanismos de revisión pública, e implementar procesos de capacitación en los sistemas de justicia y policía para mejorar la investigación y el procesamiento de tales delitos.
- Incorporar diferentes dimensiones de ciberseguridad en la preparación y revisión de los planes nacionales de acción sobre MPS (incluidos aquellos desarrollados a nivel regional y local).

Iniciativas para el desarrollo de capacidades

- Integrar las perspectivas de género en la elaboración de iniciativas, materiales y programas de formación para el desarrollo de capacidades.
- Garantizar que las mujeres tengan igual acceso a las tecnologías digitales.
- Involucrar a las mujeres y niñas en la creación y el desarrollo de contenidos.

Investigación adicional

- Recopilar datos desagregados en cuanto al género sobre el acceso y uso de las tecnologías digitales y los impactos de los ciberincidentes y ciberataques sobre diferentes comunidades para orientar nuevas investigaciones y nuevos análisis.

- Preparar casos de estudio e identificar las mejores prácticas para guiar a los Estados, las organizaciones internacionales y al sector privado para que integren mejor los enfoques sobre MPS y ciberseguridad internacional.

Estas recomendaciones tendrán relevancia para los gobiernos, las personas creadoras de políticas, el sector privado y las organizaciones de la sociedad civil. Las recomendaciones tienen aplicación en el desarrollo de políticas nacionales y regionales y en los enfoques de los Estados en la Primera Comisión de la Asamblea General y el Consejo de Seguridad. Juntos pueden forjar una agenda MPS más fuerte y un enfoque más inclusivo en las conversaciones sobre ciberseguridad internacional.

1. Introducción

La agenda MPS provee un marco útil para abordar las amenazas contra la seguridad internacional y sus dimensiones en cuanto al género, además de promover la participación de las mujeres en la toma de decisiones sobre la seguridad internacional. Hasta ahora, sin embargo, el marco MPS no ha sido aplicado sistemáticamente al ciberespacio.

Esto no es de sorprender, dado que las bases de la agenda MPS se establecieron en el 2000 mediante la resolución 1325 (2000) sobre Mujeres, Paz y Seguridad[1] del Consejo de Seguridad. En dicho momento político se puso atención particular a las formas tradicionales de conflicto pues el mundo todavía estaba conmovido por el genocidio en Ruanda y las guerras en la República Democrática del Congo, Liberia, Sierra Leona y la antigua Yugoslavia.[2]

Hasta el momento nueve resoluciones sobre MPS han seguido la resolución inicial del 2000, las cuales colectivamente forman la base de lo que a menudo se designa como la agenda MPS.[3] Estas resoluciones han establecido áreas de reforma bajo 'cuatro pilares', a saber, la participación de las mujeres en los asuntos de paz y seguridad, la inclusión de las mujeres en los esfuerzos para la prevención de conflictos, la protección de las mujeres y sus derechos y la atención de las necesidades de las mujeres durante las fases de asistencia y recuperación en casos de conflicto. También insta a las Naciones Unidas y otros actores a integrar una perspectiva de género en sus esfuerzos de paz y seguridad. No obstante, ninguna de las resoluciones sobre MPS contiene referencias a 'ciber', 'en línea', 'tecnología', 'digital' o 'Internet', ni tampoco al ciberespacio o la ciberseguridad.

Veinte años después de esa emblemática resolución, el mundo digital sustenta casi todas las estructuras y los sistemas de la vida moderna. Conforme la agenda MPS entra a su tercera década, un número cada vez mayor de actores nacionales e internacionales han estado invitando a que se integre mejor con los temas de ciberseguridad. Durante las reuniones del Grupo de Trabajo de Composición Abierta sobre el progreso de la informática y las telecomunicaciones en el contexto de la seguridad internacional (en adelante, el GTCA), entre el 2019 y el 2021, varios Estados llamaron la atención a las dimensiones del ciberespacio basadas en género, incluyendo los impactos potenciales de

género de los incidentes de las tecnologías de la información y las comunicaciones (TIC), así como también sobre la brecha global de género con respecto al acceso y uso de la Internet. La necesidad de fortalecer los vínculos entre las conversaciones sobre la seguridad de las TIC y la agenda MPS también se mencionó de manera explícita en dichas discusiones.[4]

Este estudio procura contribuir a estos esfuerzos al examinar cómo la agenda MPS puede aplicarse a las discusiones sobre seguridad internacional en el ciberespacio con el propósito de integrar mejor las consideraciones de género, fortalecer la igualdad de género y transformar nuestro enfoque hacia la paz y la seguridad internacionales ante la amenazas cambiantes y las oportunidades que plantea el ciberespacio.

El análisis presentado está anclado en un entendimiento de las amenazas de ciberseguridad basadas en género que reconoce que aquellos incidentes 'tradicionales' sobre las TIC, tales como los ataques de denegación de servicio relacionados con servicios básicos, tienen resultados marcados por el género. También reconoce que el doxeo, el ciberacoso y la distribución de imágenes íntimas sin consentimiento (la denominada 'pornovenganza') también son amenazas que pueden provenir de la intrusión de los dispositivos y redes personales o su alteración[5] o del uso malicioso de las tecnologías digitales.

Este entendimiento de la ciberseguridad representa un alejamiento de la perspectiva común que considera las amenazas contra la seguridad de las mujeres o la violencia basada en género como un problema de 'protección cibernética' y, por ende, la excluye de las discusiones sobre ciberseguridad.[6]

En vez de aislar los conceptos de 'ciberseguridad' y 'protección cibernética',[7] este entendimiento buscar tomarlos de manera holística y reconoce que la "cibertecnología ha traído una nueva elasticidad a los conceptos de las amenazas a la paz y la seguridad internacionales".[8] Este enfoque enfatiza la protección de los derechos humanos, lo cual es integral para mejorar la participación y protección de las mujeres en los entornos tanto en como fuera de línea.

Aprovechando el creciente corpus de investigación sobre género y ciberseguridad, además de investigación documental y entrevistas con representantes de Estados

(consultar la metodología en el Anexo), este trabajo articula los vínculos entre los temas prioritarios de MPS (igualdad de género, participación de las mujeres en la seguridad internacional, prevención de la violencia contra las mujeres y su protección, necesidades diferenciadas por género) y la ciberseguridad internacional.

La investigación inicia situando estas discusiones específicas dentro de los procesos multilaterales, evaluando el grado hasta el cual los temas relacionados con la informática y MPS se han considerado juntos en las negociaciones y los debates en la Primera Comisión de la Asamblea General y el Consejo de Seguridad. Luego identifica algunos desafíos claves y su relación con el ciberespacio y la paz y seguridad internacionales, vistos a través de los lentes de la agenda MPS: la participación de las mujeres en las negociaciones de ciberseguridad, la participación de las mujeres en los procesos políticos, el abuso en línea y la violencia contra las mujeres, el género y la radicalización en línea, los impactos de género de los ciberincidentes y los sesgos de género en las tecnologías digitales.[9] Finalmente, presenta recomendaciones concretas para abordar la ciberseguridad como "la siguiente frontera de la agenda MPS".[10]

Al poner las tecnologías digitales y las consideraciones de ciberseguridad en primer plano en la agenda MPS, este trabajo espera producir la muy necesaria 'actualización del sistema' y garantizar que la comunidad internacional esté equipada para lidiar con los desafíos de seguridad internacional del siglo veintiuno y sus implicaciones en cuanto al género.

Terminología

Inteligencia artificial. La inteligencia artificial se refiere a las tecnologías informáticas que intentan imitar las capacidades cognitivas y de razonamiento humano o animal con el fin de crear máquinas "inteligentes". "La inteligencia mide la habilidad de un sistema de determinar el mejor curso de acción para alcanzar sus metas en una amplia gama de entornos"; sin embargo, "el estándar para las máquinas que se consideran "inteligentes" está cambiando constantemente".[11]

Ciberseguridad se refiere a los procesos o las prácticas de protección de sistemas, redes y otras TIC contra ataques maliciosos, además de prevenir su mal uso, abuso o manipulación para causar daño a otras personas.

Ciberespacio se refiere tanto a la Internet como a las TIC que conectan, usan y dependen de la Internet, tales como computadoras, teléfonos inteligentes y otros dispositivos con conexión a la Internet.[12]

Género se refiere a los roles, las conductas, las actividades y los atributos que una sociedad dada en un momento dado considera apropiados o como una 'norma' para las mujeres y los hombres y las niñas y los niños, así como también para las personas de género no binario o género fluido.

Las normas de género son diferencias construidas socialmente – distintas a las diferencias biológicas (sexo) — y funcionan como reglas sociales de conducta, estableciendo lo que es deseable y posible de hacer como un ser masculino o femenino en un contexto dado.[13]

Análisis de género es un análisis crítico de cómo las diferencias en los roles, las actividades, las necesidades, las oportunidades y los derechos y las prerrogativas en cuanto al género afectan a hombres, mujeres, niñas, niños, personas de género no binario o fluido en ciertas situaciones o contextos. El

análisis de género examina las relaciones entre los géneros y su acceso a los recursos y su control y las restricciones que enfrentan unos en comparación con los otros.[14]

Tecnologías de la información y comunicación (TIC) se refiere a los programas, las redes y los dispositivos que crean, almacenan y transmiten datos electrónicamente.

Resolución 1325 (2000) sobre Mujeres, Paz y Seguridad del Consejo de Seguridad la resolución 1325 (2000) sobre mujeres, paz y seguridad del Consejo de Seguridad reafirma el importante papel de las mujeres en la prevención y resolución de conflictos, las negociaciones de paz, la construcción y el mantenimiento de la paz, la respuesta humanitaria y la reconstrucción post conflicto. Enfatiza la importancia de su participación equitativa y plena en todos los esfuerzos para mantener y promover la paz y la seguridad. Insta a todos los actores a aumentar la participación de las mujeres e incorporar las perspectivas de género en todos los esfuerzos de paz y seguridad de las Naciones Unidas. También invita a todas las partes de un conflicto a tomar medidas especiales para proteger a las mujeres y niñas contra la violencia basada en género, particularmente la violación y otras formas de abuso sexual, en situaciones de conflicto armado.[15]

2. Posicionamiento de la agenda MPS y los procesos de ciberseguridad internacional dentro de las Naciones Unidas

Con el fin de fortalecer los vínculos entre MPS y la política de ciberseguridad internacional es importante entender cómo estas diferentes agendas han evolucionado y qué esfuerzos se han hecho para cerrar las brechas. Esto requiere un enfoque dual. Primero, entender el grado hasta el cual las tecnologías digitales y la ciberseguridad han sido abordadas como parte de la agenda MPS, particularmente dentro del Consejo de Seguridad y como parte de los planes de acción regionales, nacionales y locales sobre MPS. Y, segundo, entender los esfuerzos (y sus restricciones relacionadas) para integrar los temas prioritarios de MPS y las consideraciones de igualdad de género en las conversaciones multilaterales sobre seguridad de las TIC, particularmente en los Grupos de Personas Expertas Gubernamentales (GEG) y el GTCA sobre TIC y seguridad internacional.

2.1 ¿Hasta qué punto se han abordado las tecnologías digitales y la ciberseguridad como parte de la agenda MPS?

Los cimientos de la agenda MPS se colocaron hace más de dos décadas con la adopción de la resolución 1325 (2000). Esta resolución reconoció que el impacto de los conflictos sobre las mujeres y el papel de las mujeres en la prevención de conflictos había pasado desapercibido por mucho tiempo. Desde entonces, se han adoptado nueve resoluciones adicionales sobre MPS que han desarrollado y ampliado aún más esta agenda.[16]

La agenda MPS, según ha sido enmarcada por las resoluciones del Consejo de Seguridad, se ha enfocado en entornos en conflicto y post conflicto; sin embargo, las académicas feministas y varios Estados han procurado fomentar la aplicación de la agenda de manera más amplia,[17] a pesar de la resistencia de algunos de los miembros del Consejo.[18] Un componente central de estos argumentos ha sido también la importancia de apoyar la capacidad de acción de las mujeres y entender su propias percepciones de seguridad, que con frecuencia han sido ignoradas en la construcción de paradigmas tradicionales de seguridad,[19] a menudo debido a su falta de representación en estas conversaciones sobre seguridad.

Es de notar que el Consejo de Seguridad no ha hecho referencia al ciberespacio en el contexto de MPS en las dos últimas décadas.[20] Ninguna de las resoluciones sobre MPS

contiene referencias a 'ciber', 'en línea', 'tecnología', 'digital' o 'Internet' ni a ciberespacio o ciberseguridad. Al revisar los debates abiertos del Consejo de Seguridad sobre MPS detectamos que en los últimos 20 años los Estados y otros expositores han vinculado la agenda, la Internet o el uso de la tecnología en sus declaraciones en menos de dos docenas de ocasiones — un número relativamente pequeño considerando la alta tasa de participación de los Estados en estos debates.[21] Cuando se han hecho referencias indirectas, estas han tendido a enfocarse en dos aspectos: el uso de las TIC para habilitar los derechos de las mujeres y su participación política y el uso de las TIC con el propósito de abusar o cometer violencia contra las mujeres.

Al principio las discusiones dentro del Consejo tendían a enfocarse en habilitar la participación de las mujeres en los procesos electorales y la vida cívica mediante las TIC. Antes del 2015, unas cuantas declaraciones hicieron referencia a cómo las TIC se estaban usando para crear conciencia sobre el valor de la participación de las mujeres en los procesos políticos, el papel de las TIC como un portal para conectar a las constructoras de paz y a la tecnología como una herramienta para el desarrollo de capacidades entre las mujeres que participaban en campañas electorales.[22] También hubo algunas referencias que reflexionaban sobre el valor de las TIC en términos de las alertas tempranas, la protección de las mujeres y las denuncias de violaciones.[23] Las declaraciones generalmente se enfocaban en algunas de las oportunidades que las TIC presentaban para fortalecer la participación política de las mujeres y sus protección potencial contra los peligros.

El enfoque de las declaraciones empezó a cambiar a partir del 2015. Aunque todavía se discutían las oportunidades que las TIC brindaban en términos de apoyo a la participación de las mujeres y su protección, los Estados también empezaron a expresar sus preocupaciones sobre los riesgos asociados con los daños que tales plataformas facilitaban contra las mujeres. Algunos Estados expresaron sus preocupaciones sobre el aumento en el extremismo violento y las 'nuevas tecnologías de la información', la trata sexual de mujeres y niñas facilitada por las TIC y el troleo y los ataques en línea contra mujeres periodistas.[24] La referencia más completa sobre el potencial de las amenazas provenientes del ciberespacio en cuanto a género durante un debate sobre MPS la hizo Kenia en el 2017 al reconocer que no había suficiente investigación sobre "las formas emergentes y la dinámica del cibercrimen y los delitos impulsados por la tecnología, incluyendo la violencia electrónica contra las mujeres, la cual se está volviendo más

prevalente".[25]

Los informes resumidos sobre MPS del Grupo Informal de Personas Expertas del Consejo de Seguridad muestran un patrón similar de consideraciones limitadas de la ciberseguridad o las TIC.[26] La única referencia al ciberespacio, o al entorno en línea y digital, se hizo durante una reunión del Grupo para responder a la pandemia del coronavirus en abril del 2020 que indicó que el acceso a las herramientas digitales era crucial para la participación de las mujeres en las negociaciones de paz y el cese a los conflictos.[27]

Al revisar los informes anuales de MPS presentados por la Secretaría General ante el Consejo es posible identificar referencia a las oportunidades y amenazas presentes en los entornos en línea y digitales. Por ejemplo, en el informe del 2015 sobre MPS de la Secretaría General se hizo referencia frecuente al potencial de las nuevas tecnologías como herramientas potentes, tanto en contextos en conflicto como los ajenos al conflicto.[28] Desde el 2015, los informes de la Secretaría General han abordado temas relacionados con el impacto diferenciado en cuanto al género en el entorno en línea pero de forma limitada, enfocándose principalmente en el uso de las tecnologías para perpetuar la exploración sexual y la violencia.[29]

El informe de la Secretaría General sobre MPS del 2020 reconoció la importancia de la inclusión digital para atender las brechas de género en el acceso a la tecnología y el poder, particularmente en el contexto de los procesos de paz.[30] También reconoció que las mujeres líderes "enfrentan acoso, amenazas y abuso, tanto en la sociedad como en línea".[31] El informe además incluyó una discusión sobre los vínculos entre la agenda de desarme y MPS, reconociendo que estos no se han explorado a cabalidad y que las mujeres siguen estando subrepresentadas en las reuniones multilaterales sobre desarme.[32] No obstante, ninguno de estos informes hace referencia directamente al 'ciberespacio', la 'ciberseguridad' o la 'seguridad de las TIC'. Una mayor discusión o un análisis más profundo del nexo entre las TIC y MPS en un informe de la Secretaría General podría promover una mayor difusión del tema en las declaraciones ante el Consejo, lo cual tendría el efecto de volverlo una norma.

Más allá del Consejo de Seguridad, uno de los vehículos para la implementación de la agenda MPS han sido los 'Planes de Acción Nacionales' (PAN) y los 'Planes de Acción

Regionales' (PAR). Al momento de redactar este trabajo, 98 países habían adoptado PAN, y 11 PAR se habían puesto en práctica. La revisión de estos documentos también revela el alcance limitado de la integración de los temas informáticos en la agenda MPS.[33] Solo dos PAN mencionan las ciberamenazas: los PAN de Irlanda y Namibia de 2019.

El PAN del 2019 de Namibia (2019) denota la necesidad de "confrontar los problemas emergentes … tales como … la ciberseguridad] y por lo demás reconoce dos tipos específicos de peligros provenientes de amenazas en el dominio cibernético: el cibercrimen y los delitos basados en género facilitados por medios cibernéticos.[34] El PAN del 2019 de Irlanda (2019) también denota que estos son nuevos desafíos para la paz y la seguridad internacionales e invita al gobierno irlandés a apoyar el cierre de la brecha de género en los empleos en ciberseguridad. Es el único punto de acción directa en cualquier PAN para atacar el problema de participación en este espacio.[35]

2.2. ¿Hasta qué punto las prioridades sobre MPS han sido abordadas en las discusiones sobre la ciberseguridad internacional?

Desde 1998, cuando la Federación Rusa presentó una resolución sobre las TIC en el contexto de la seguridad internacional, la Primera Comisión de la Asamblea General ha trabajado en temas relacionados con la ciberseguridad.[36] La adición de este tema a la agenda de la Primera Comisión inicialmente fue recibida con desacuerdo y escepticismo de parte de algunos Estados.[37] Estaban en desacuerdo con conceptos claves de la seguridad de la información (por ejemplo, si la información misma es un arma), si se necesitaban nuevas normas internacionales y el papel de la Primera Comisión en las discusiones sobre la seguridad de la información internacional.[38] A pesar de este escepticismo inicial, la Primera Comisión ha surgido como un jugador clave en las discusiones sobre la ciberseguridad.

En el 2003, la Primera Comisión aprobó el establecimiento de un GEG para examinar conceptos internacionales relevantes con miras a fortalecer la seguridad de los sistemas globales de las TIC.[39] El grupo, que constó de personas expertas de 15 Estados, se reunió en tres ocasiones en el curso de un año. Desde entonces, otros cinco GEG han sido establecidos por la Asamblea General para continuar el estudio y la discusión de temas

tales como la aplicabilidad del derecho internacional al ciberespacio, la cooperación internacional y las amenazas existentes y potenciales.

No hay referencia a 'mujeres', 'niñas' ni a 'género' en los tres informes que fueron adoptados por consenso por el GEG en el 2010, 2013 y 2015.[40] Aunque estos informes del GEG incluyen referencias a respetar "los derechos humanos y las libertades fundamentales" y a "la privacidad y libertad de expresión", no hay referencias a los peligros potenciales ni a los abusos de los derechos provenientes del diseño y la utilización de las TIC.

Además, no se trazan vínculos hacia la importancia de la participación de las mujeres en la ciberseguridad ni hacia la importancia del análisis de género para entender cómo la seguridad de las TIC puede contribuir a la paz y la seguridad internacionales o volverse una amenaza contra ellas. Sin embargo, se hizo algún progreso en el GEG del 2021 con una referencia al género y la reducción de la brecha digital.[41]

Mediante la resolución 73/27, la Asamblea General estableció un GTCA al cual se invitó a todos los Estados Miembro a participar.[42] A diferencia de los GEG que tienen una membrecía limitada y se reúnen a puerta cerrada, el GTCA se diseñó como un proceso inclusivo y transparente. Durante las reuniones del 2019, 2020 y 2021 del GTCA, varias delegaciones llamaron la atención a los impactos potenciales en cuanto al género de los incidentes con las TIC, así como también a la brecha global de género con respecto al acceso y uso de la Internet.[43] Un documento de trabajo presentado ante el GTCA propuso que la igualdad de género y la participación significativa de las mujeres debería estar en el corazón de la paz y la seguridad internacionales en el ciberespacio.[44] Una nueva investigación que exploraba cómo las normas de género dan forma a actividades específicas relacionadas con la ciberseguridad fue presentada en eventos paralelos y múltiples organizaciones de la sociedad civil resaltaron la importancia de incorporar el género en las políticas sobre la informática.[45]

Adoptado por consenso en marzo del 2021, el informe final del GTCA reconoció el alto nivel de participación femenina en sus sesiones, así como también la relevancia de las perspectivas de género en sus discusiones y resaltó la importancia de reducir la "brecha digital de género" y promover la participación eficaz y significativa y el liderazgo de las mujeres en los procesos de toma de decisiones. Asimismo, el informe final propuso que

los esfuerzos para el desarrollo de capacidades deberían "respetar los derechos humanos y las libertades fundamentales, ser sensibles e inclusivos en cuanto al género, universales y no discriminatorios".[46]

Sin embargo, el Grupo no pudo llegar a un consenso sobre un lenguaje que describiera la profundidad de las discusiones y el rango de perspectivas presentadas.[47] Por ello, la Presidencia emitió su propio resumen de las discusiones, el cual reflejó la amplitud de las consideraciones que hicieron los Estados sobre temas relacionados con género. Por ejemplo, algunos Estados enfatizaron las interrelaciones entre las normas, la generación de confianza y el desarrollo de capacidades y destacaron la necesidad de que las perspectivas de género se incorporaran a la implementación de las normas. Algunos Estados llamaron la atención a la "brecha digital de género" e instaron a que se tomaran medidas específicas tanto a nivel nacional como internacional para abordar la equidad de género y la participación significativa de las mujeres en las conversaciones internacionales y los programas de desarrollo de capacidades sobre las TIC y la seguridad internacional, incluyendo la recopilación de datos desagregados por género. Los Estados expresaron su aprecio por los programas que han facilitado la participación de las mujeres en las conversaciones multilaterales sobre seguridad de las TIC. También se enfatizó la necesidad de fortalecer los vínculos entre este tema y la agenda MPS.[48]

El lenguaje incorporado en el Informe Final del GTCA del 2021 y el Resumen de la Presidencia demuestran el avance más sustancial dentro de los procesos multilaterales de las Naciones Unidas hasta la fecha con respecto a la vinculación de las agendas MPS y de ciberseguridad internacional, incluyendo la necesidad de integrar las perspectivas de género. Sin embargo, en buena medida fue un texto conciliador.[49]Parte del lenguaje propuesto más fuerte no fue incluido en las conclusiones y recomendaciones y no se exhortó a la acción. En última instancia, el lenguaje incluido en borradores anteriores que instaba a la acción para abordar la 'brecha digital de género', recopilar datos desagregados por género, atender la desigualdad de género y la participación significativa de las mujeres y reconocer la necesidad de fortalecer los vínculos entre la agenda MPS y las discusiones multilaterales sobre la seguridad de las TIC no logró el consenso de todos los Estados.

A diferencia de la Primera Comisión de la Asamblea General, el Consejo de Seguridad hasta hace poco ha empezado a considerar el tema de las ciberamenazas y sus

implicaciones para la paz y la seguridad internacionales. Las discusiones sobre las ciberamenazas se han enfocado en varias reuniones (informales) realizadas con arreglo a la "fórmula Arria" del Consejo desde el 2016.[50]Algunos Estados han utilizado el formo de las reuniones con arreglo a la fórmula Arria para delinear los vínculos entre aspectos de la agenda MPS y la ciberseguridad. Esto ha incluido el reconocimiento de la importancia de la paridad de género en las intervenciones y la participación de las mujeres en iniciativas de desarrollo de capacidades cibernéticas,[51] el desarrollo de capacidades sensibles al género,[52] el cierre de la brecha digital para satisfacer los Objetivos de Desarrollo Sostenible,[53] reflexionar sobre los vínculos entre MPS y el ciberespacio[54] y reconocer el impacto diferenciado que los ciberataques sobre la infraestructura crítica tienen sobre la mujeres y niñas.[55]

El Consejo organizó su primer debate formal abierto sobre la paz y seguridad internacionales en el ciberespacio en junio de 2021 cuando la presidencia estaba a cargo de Estonia. En dicho debate, la Alta Representante para Asuntos de Desarme reconoció que las amenazas de las TIC tienen un impacto en cuanto al género y que esta era la razón por la cual tanto mujeres como hombres necesitaban participar en "la toma de decisiones en la arena digital".[56] No obstante, hubo poca discusión entre los Estados sobre las diferentes dimensiones de la ciberseguridad respecto al género. Los vínculos entre la ciberseguridad y MPS aún no han florecido en las consideraciones que hace el Consejo sobre cuáles puntos a incluir en su agenda.

3. Actualización del sistema: áreas claves de acción

Con el fin de reducir la brecha en MPS y ciberseguridad, este informe identifica seis desafíos que deben ser abordados. Llevar estas consideraciones a primer plano en la agenda MPS y las discusiones sobre ciberseguridad internacional producirá una muy necesaria 'actualización del sistema' y asegurará que la comunidad internacional esté equipada para lidiar con los desafíos de seguridad internacional del siglo veintiuno.

3.1 Participación de las mujeres en las negociaciones de ciberseguridad

La agenda MPS busca lograr la participación eficaz y significativa de las mujeres en todo el espectro de la seguridad internacional. Varios Estados y actores multilaterales han reconocido la importancia de alcanzar esta meta en las negociaciones internacionales y en la toma de decisiones sobre temas informáticos también.[57] En las entrevistas realizadas para este proyecto, con frecuencia se mencionó la participación de las mujeres somo el asunto más fácilmente identificable en cuanto a la integración del género en la ciberseguridad. Las personas entrevistadas enfatizaron este aspecto como un tema de igualdad de género y derechos humanos, además de un factor de diversidad que podría traer beneficios a las conversaciones y negociaciones.[58]

Sin embargo, las mujeres continúan estando subrepresentadas en las negociaciones multilaterales de ciberseguridad, constituyendo, en promedio, un tercio de las personas delegadas acreditadas ante la Primera Comisión.[59] Este es un marcado contraste con la Tercera Comisión que trata temas sociales, humanitarios y culturales, donde casi el cincuenta por ciento de las personas delegadas son mujeres.[60] Aún más patente es el desbalance de género en los grupos más pequeños y grupos de trabajo que tratan con temas de seguridad internacional, tales como el GEG sobre las TIC. En promedio de los seis GEG, las mujeres representan únicamente un 20 por ciento de las personas expertas nominadas por los gobiernos.[61]

Como respuesta al compromiso establecido bajo el auspicio de la Secretaría General de alcanzar la paridad de género en los órganos sobre desarme, la composición del GEG del 2019 incluyó 15 hombres y 10 mujeres.[62]

En un esfuerzo para apoyar la participación significativa de las mujeres en las

discusiones multilaterales sobre temas relacionados con las TIC en el contexto de la seguridad internacional, en el 2019 los gobiernos de Australia, Canadá, los Países Bajos, Nueva Zelanda y el Reino Unido establecieron un programa de becas titulado Women in International Security and Cyberspace Fellowship.[63] Como parte de este programa, 35 mujeres recibieron becas para asistir a las reuniones de GTCA en Nueva York y para capacitarse en negociaciones multilaterales en el Instituto de las Naciones Unidas para la Formación Profesional e Investigaciones.[64] Luego de las sesiones de capacitación del programa, hubo un aumento notable en el nivel de involucramiento de las mujeres en el GTCA sobre TIC en el Contexto de la Seguridad Internacional, pues más de un 40 por ciento de las declaraciones oficiales en la segunda sesión sustantiva fueron presentadas por mujeres.[65]

Asimismo, el informe final del GTCA reconoció la importancia de la participación de las mujeres en los procesos de toma de decisiones sobre las TIC en la seguridad internacional.[66] Sin embargo, el informe del GTCA no fue más allá de instar a los Estados a tomar acciones para abordar la participación significativa de las mujeres en las discusiones de ciberseguridad y los programas de desarrollo de capacidades. Esto muestra que todavía se puede hacer más en cuanto a las acciones, el compromiso y la investigación para entender la participación de las mujeres y garantizar que estas tengan las oportunidades de participar de manera significativa en los procesos de ciberseguridad e influir en ellos.

La participación de las mujeres en la toma de decisiones sobre la ciberseguridad internacional es transcendental pues puede ser una vía para disminuir la desigualdad de género al ofrecer una diversidad de perspectivas que podría permitir que la información sea procesada con más cuidado y que se tomen mejores decisiones sobre las políticas.[67]

Sobre todo, las mujeres están en una mejor posición "de identificar sus necesidades particulares en cuanto a la ciberseguridad y aportar sus experiencias a la base de conocimientos y así orientar la ciberseguridad".[68] Los esfuerzos para aumentar la participación de las mujeres también deben complementarse con "la incorporación activa de las perspectivas de género en las políticas y los programas",[69] que apoyan un enfoque más integral para promocionar la agenda MPS como parte de la ciberseguridad.

3.2 La ciberviolencia contra las mujeres y niñas

La prevención de todas las formas de violencia que afectan a las mujeres y niñas y su protección contra estas están en el corazón de la agenda MPS. Las TIC han provisto a las mujeres diferentes herramientas para movilizarse e interactuar con aplicaciones en línea que comparten información sobre las amenazas contra su seguridad. Por ejemplo, hay ejemplos de mujeres que utilizan las tecnologías digitales para compartir información y mapear sus preocupaciones de seguridad para aumentar su protección y apoyar los mecanismos de alerta temprana en áreas afectadas por conflictos.

No obstante, el entorno virtual también ha expuesto a las mujeres a un nivel desproporcionado de violencia y abuso en los espacios digitales. Las mujeres de todos tipos, desde políticas hasta defensoras de los derechos humanos y usuarias particulares, enfrentan acoso y amenazas en línea que, en algunos casos, han llevado a ataques contra su seguridad física. Por lo tanto, proteger a las mujeres y niñas contra la ciberviolencia tiene que ser parte de la agenda MPS también.[70]

En algunos casos, se usan ataques y campañas de acoso dirigidas particularmente en las redes sociales para silenciar a las mujeres en espacios públicos y comunidades.[71]A veces, el acoso en línea muta hacia violencia armada, tal como en el caso de la radicalización en línea de los 'incels'. También conocidos como 'célibes involuntarios', los incels son parte de una subcultura de supremacía masculina, racista, misógina virulenta que se manifiesta de más manera más visible en línea. Si bien, , autoproclamados incels también han cometido actos de violencia, principalmente tiroteos.[72]

Los espacios virtuales y el Dark Web se pueden utilizar para perpetuar la violencia contra las mujeres, incluyendo actos criminales como la trata de personas. La explotación sexual y el abuso en línea a menudo son acompañados por violencia física contra las mujeres y niñas o llevar a esta.[73] Igualmente, los cierres y las restricciones de viajes impuestos por la pandemia del COVID 19 produjeron un repunte en la explotación sexual y el abuso en línea contra las mujeres y niñas, incluida la explotación sexual comercial, y un incremento en las personas que intentaban tener acceso a páginas web ilegales que presentaban material de abuso sexual contra niñas.[74]

Para captar las muchas formas de ciberviolencia contra las mujeres y niñas, la red Violence Against Women Learning Network identificó seis amplias categorías (vea la Tabla 1).[75]

Tabla 1. Ciberviolencia contra mujeres y niñas

Piratería informática (Hacking)	Uso de la tecnología para tener acceso ilegal y no autorizado a sistemas o recursos con el propósito de conseguir información personal, alterar o modificar información o calumniar e insultar a la víctima o las organizaciones que representan.
Suplantación de personalidad	Uso de la tecnología para asumir la identidad de la víctima o alguien más con el fin de tener acceso a información privada, avergonzar o humillar a la víctima, contactar a la víctima o crear documentos de identidad fraudulentos.
Vigilancia / Rastreo	Uso de la tecnología para acechar y monitorear las actividades y conductas de una víctima ya sea en tiempo real o históricamente.
Acoso	Uso de la tecnología para contactar, molestar, amenazar y asustar continuamente a la víctima. Este es un comportamiento continuo y no un incidente aislado.
Reclutamiento	Uso de la tecnología para seducir a víctimas potenciales para que caigan en situaciones violentas.
Distribución maliciosa	Uso de la tecnología para manipular y distribuir materiales difamatorios e ilegales relacionados con la víctima u organizaciones de mujeres.

La violencia en línea y fuera de línea se alimenta una a la otra. Proteger a las mujeres y niñas contra la ciberviolencia es una parte integral de la agenda MPS y debería incluirse en los planes de acción nacionales y regionales para implementar la resolución 1325 (2000). Esto requerirá que los Estados ajusten la manera en que abordan los asuntos que tradicionalmente han estado enmarcados como preocupaciones internas (por ejemplo, los peligros humanos de la violencia facilitada por la informática) en los planes de acción nacionales de MPS, en vez de enfocarse solamente en las amenazas contra la seguridad externas.[76] Igualmente, este problema de la ciberviolencia debería abordarse también en la legislación nacional, pues podrían necesitarse nuevas leyes para actualizar la definición de lo que es la ciberviolencia para incluir los diferentes tipos de abuso y violencia facilitados por las tecnologías contra las mujeres y niñas.

3.3 Participación de las mujeres en procesos políticos

La brecha digital de género es evidente en la mayor parte del mundo pues los hombre jóvenes de los países occidentales tienen muchas más probabilidades de tener acceso a la Internet que las mujeres de las economías emergentes.[77] En el 2015, el Estudio Global sobre la implementación de la resolución 1325 (2000) reconoció que las barreras para el acceso de las mujeres a la tecnología podrían limitar su empoderamiento.[78] Tales barreras también pueden restringir su participación en la vida cívica. En vista de esto, la Secretaría General ha hecho un llamado por "iniciativas de inclusión digital" para atender las brechas de género y fortalecer los mecanismos para "involucrar significativamente a todos los constituyentes".[79]

Aunque las TIC abren la puerta a las oportunidades para el involucramiento en organizaciones base con una mayor gama de individuos y la formación de comunidades en línea, también facilitan el abuso y acoso por parte de individuos, grupos e incluso actores estatales. Dicho abuso en línea puede disuadir a las mujeres de participar en los procesos políticos, particularmente de ser candidatas a puestos políticos. El Informe sobre Mujeres, Paz y Seguridad de la Secretaría General del 2019, por ejemplo, señala que las candidatas a elecciones enfrentan intimidación y acoso en línea en varios países.[80] Dicho acoso puede actuar como una barrera para la participación de las mujeres en la política.[81]

La naturaleza anónima del entorno virtual, aunado a los algoritmos de las plataformas de las redes sociales, puede facilitar la diseminación rápida de información errónea y desinformación. Las campañas de desinformación sexualizada y basada en género — lideradas por actores estatales en algunos casos — pueden socavar la credibilidad de las mujeres y el éxito de sus campañas políticas en estos contextos.[82]

Una forma de desinformación basada en género que ha sido utilizada son los 'deepfakes'. Los deepfakes son falsificaciones digitales (imágenes, videos y audios) creados mediante aprendizaje profundo, un subconjunto de la inteligencia artificial (IA).[83] Los deepfakes replican el aspecto y sonido del habla humana y los movimientos humanos reales, permitiendo a los usuarios crear videos realistas de personas haciendo y diciendo cosas que nunca hicieron ni dijeron.[84] Se pueden usar para campañas de difamación y desprestigio en línea,[85] e incluso para silenciar a las defensoras de los derechos de las mujeres mediante intimidación y miedo de sufrir violencia sexual y violencia basada en género.[86] Los videos deepfakes que circulan en línea no solo pueden socavar la participación política de las mujeres, sino que también de manera más general representan un problema de seguridad en cuanto al género.[87]

La participación de las mujeres en la política y en las instituciones gubernamentales es central para los esfuerzos de fortalecer la representación femenina y potenciar sus voces y promover aún más los esfuerzos para robustecer la agenda MPS. Sin embargo, la facilidad con la cual las TIC permiten que las mujeres sean intimidadas, acosadas y denigradas en línea significa que las mujeres continuarán enfrentando barreras adicionales para participar en los procesos políticos. Aunque todavía hace falta investigar el impacto de la intimidación y el acoso digitales sobre las candidatas, podría ser un patrón de abuso con la intención de intimidar a las mujeres y evitar que participen en la vida política.

3.4 Género y radicalización en línea

Los grupos terroristas y extremistas han utilizado el ciberespacio para promover narrativas misóginas con el fin de formar comunidades y radicalizar individuos, lo cual amenaza la seguridad internacional y los objetivos de la agenda MPS.[88] Algunas organizaciones terroristas han sido muy eficaces en la aplicación del lente de género en

sus programas de reclutamiento para capitalizar el involucramiento de hombres y mujeres.

El Estado Islámico en Iraq y el Levante (ISIS), por ejemplo, promueve narrativas muy sexistas y roles masculinos y femeninos 'idealizados' en sus estrategias de reclutamiento.[89] Como las investigaciones han mostrado, los grupos terroristas son "más activos y avanzados en su pensamiento sobre el género que la comunidad internacional contra el terrorismo".[90]

En el caso del reclutamiento de ISIS, la investigación ha determinado que las mujeres estaban en mayor riesgo de ser radicalizadas y reclutadas en línea que fuera de línea.[91] Esto también podría tener un impacto sobre el grado hasta el cual diferentes grupos de personas son radicalizadas, dependiendo de su acceso a la Internet, y las estructuras de poder en la sociedad. La investigación igualmente ha indicado que, una vez reclutadas, los roles de las mujeres incluyen principalmente compartir propaganda y material de reclutamiento y recaudar fondos en línea, todas actividades que facilitan que la violencia física sea perpetrada por estos grupos.[92]

El uso de la Internet para diseminar una ideología y radicalizar a los individuos ha "aumentado exponencialmente el grupo de miembros potenciales" y los blancos de estas organizaciones extremistas.[93] Los ataques perpetrados por terroristas de ultra derecha en los últimos años notablemente han estado 'centrados en la Internet' en el sentido que fueron planeados y divulgados en línea.[94] No obstante, las influencias en cuanto al género y los impactos de la retórica de la extrema derecha en línea siguen sin ser explorados en la literatura y las discusiones de los Estados.[95] Entender el atractivo diferente de estas plataformas y la participación en ellas según el género es clave para abordar algunos de los riesgos que plantean para la paz y la seguridad con el fin de evitar la radicalización de individuos por medio de estas plataformas y responder a ello.

Restringir la diseminación del contenido terrorista sigue siendo responsabilidad de las empresas de redes sociales y tecnología, aunque ese papel cada vez más está siendo regulado mediante leyes nacionales. Los enfoques difieren entre las plataformas, lo cual permite a los individuos escoger cómo hacerlo. Algunos sitios de redes sociales, tales como Twitter y Facebook, han tomado pasos para desactivar cuentas y remover contenido cuando alcanza un umbral de preocupación, pero a menudo esto llega muy

tarde. Incluso cuando ocurre, las comunidades vedadas simplemente migran a plataformas con menos moderación o crean nuevas cuentas.[96] También hay preocupación de que medir el potencial del contenido terrorista puede enmarcarse como una manera de restricción de los derechos humanos y la libertad de expresión, lo cual podría tener un impacto en la movilización y la participación política de las mujeres.

Se necesita un diálogo multiparticipativo, que incluya a los Estados, la sociedad civil, las empresas de plataformas tecnológicas y de redes sociales para generar maneras eficaces de restringir la diseminación de contenido terrorista y la desinformación en línea.[97] Conocer la dinámica de género probablemente potenciaría la eficacia de tales iniciativas, las cuales, hasta ahora, han sido diseñadas de una manera "ciega" a las cuestiones de género.[98]

3.5 Impactos de los ciberincidentes en cuanto al género

La resolución 1325 (2000) reconoce los impactos de los conflictos en cuanto al género y que las necesidades de seguridad de las mujeres y niñas son diferentes. Muy parecido al conflicto tradicional, el uso de las TIC por actores estatales y no estatales puede tener impactos diferentes sobre los hombres y las mujeres.[99] Por ejemplo, las mujeres a menudo dependen de sus móviles y comunicaciones en línea para manejar su seguridad. El corte de la Internet mediante apagones podría privarlas de estas herramientas. Asimismo, las oportunidades de educación, los beneficios económicos y la seguridad personal de las mujeres pueden ser impactados cuando ocurren apagones de la Internet.[100]

Igualmente, las filtraciones de datos pueden tener un impacto desproporcionado sobre las mujeres. Un ejemplo presentado por Brown & Pytlak (2020) se refiere a una filtración de datos que ocurrió en Sao Paulo, Brasil, en julio del 2016. Se expusieron los registros de salud de 650.000 pacientes, incluyendo información sobre embarazos y atención de abortos. El aborto es ilegal en ciertas circunstancias en Brasil, lo que significa que los derechos de las mujeres tenían probabilidad de ser impactados de manera diferente por esta filtración de datos y potencialmente podría exponerlas a

acusaciones penales.[101] El no considerar los impactos diferenciados según el género de estos incidentes podría significar que tales eventos no sean considerados como una amenaza como otros ciberincidentes.

La recopilación constante de datos desagregados por género por la sociedad civil e investigadores cuando suceden estos eventos, incluyendo el análisis de cómo hombres, mujeres, personas identificadas como no binarios y diferentes comunidades se ven afectadas, puede propiciar respuestas políticas más efectivas cuando ocurren estos eventos, fortaleciendo así el apoyo al socorro y la recuperación de las mujeres después del incidente.

Se requiere más investigación para examinar el impacto diferenciado por género de los instrumentos de políticas de ciberseguridad (tal como los apagones de la Internet), las filtraciones de datos y los ataques sobre infraestructura crítica. Los Estados deberían también procurar incorporar perspectivas de género en el desarrollo de sus políticas sobre la protección de la infraestructura crítica, incluyendo el cómo enmarcan y definen lo que es una 'infraestructura crítica' y una 'infraestructura con información crítica' y la prioridad asignada a diferentes tipos de incidentes.

3.6 Sesgos sobre género en las tecnologías digitales

La tecnología refleja y, al mismo tiempo, da forma a la sociedad que la crea. En consecuencia, la tecnología incorpora y, a veces, perpetúa la desigualdad de género y otras inequidades estructurales que ya existen dentro de una sociedad dada. La raza humana es la primera fuente de prejuicios, lo cual influye directamente en los datos de entrada usados para poner a prueba y entrenar los algoritmos. Incluso los grandes procesos automatizados dependen de juicios 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.[102] El resultado a menudo es que se insertan supuestos en cuanto al género y datos sesgados en los algoritmos.[103]

La investigación ha mostrado que los modelos de amenazas, los procedimientos de

notificación y control de las personas usuarias y la publicidad de las tecnologías de ciberseguridad significan que las mujeres tienen más probabilidad de restar importancia a las amenazas u omitirlas, de tener cargas adicionales de seguridad y de ser afectadas por el mercadeo engañoso sobre ciberseguridad.[104] Por ejemplo, el diseño de los dispositivos domésticos inteligentes no ha incluido adecuadamente la violencia de pareja en la fase de diseño del 'modelado de amenazas', lo cual significa que los supuestamente seguros dispositivos inteligentes aumentan los riesgos relacionados con el género.[105]

Por ende, para reducir la ocurrencia de estos puntos ciegos peligrosamente inadvertidos es importante que los procesos de diseño y modelado de amenazas incluyan diversas perspectivas y personas de los grupos minoritarios.[106]

Una fuerza laboral diversa en cuanto al género podría ser un medio para evitar tales puntos ciegos. De acuerdo con el Informe global de la brecha de género del 2018 del Foro Económico Mundial, las mujeres representan menos de una cuarta parte de los profesionales en IA en el mundo.[107] Esta disparidad en la fuerza laboral ha levantado preocupaciones sobre la reproducción y el reforzamiento de los sesgos dentro de los sistemas de IA, tal como "los estereotipos de género y las normas sociales discriminatorias existentes".[108]

Existe evidencia de que algunos de los algoritmos que se ponen en práctica en los sistemas de justicia penal podrían producir sentencias desproporcionadas para las mujeres y otros grupos minoritarios debido a las predicciones sobre las tasas de reincidencia basadas en datos sesgados.[109] Los sesgos en tales algoritmos podrían también plantear desafíos en términos de la ciberseguridad cuando se trata del uso malicioso e invasión de los sistemas. El software para evitar la intrusión de actores maliciosos a menudo depende de algoritmos que identifican patrones. Aunque se argumenta que tales procesos pueden aumentar la habilidad de los seres humanos de identificar las amenazas y responder a ellas, estos podrían estar viciados si los datos de los cuales dependen incluyen ciertos supuestos sobre los infractores (esto es, que son hombres).

Los sesgos en los conjuntos de datos y entre la fuerza laboral informática y de IA plantean preguntas sobre los escenarios o las situaciones donde se podría aplicar la IA dentro del dominio de la seguridad en cuanto a armas autónomas (que son activadas

mediante plataformas en línea) o los procesos y algoritmos para la toma de decisiones. La naturaleza emergente de estos desarrollos tecnológicos significa que se requiere más investigación para explorar estos retos. También hay una pregunta pendiente en la investigación sobre si las tecnologías digitales que refuerzan las desigualdades de género en la sociedad podrían contribuir a las condiciones que facilitan el conflicto dentro de un país o que predicen una agresión al Estado, en la misma manera que otros indicadores sugieren la existencia de este vínculo.[110]

4. Conclusiones: hacia una agenda sobre Mujeres, Paz y Ciberseguridad

El mundo digital sustenta cada estructura y sistema de la vida moderna. El ciberespacio ofrece oportunidades para promover la agenda MPS, pero también plantea amenazas contra el empoderamiento y la seguridad de las mujeres. Aún así, como se ha demostrado en este trabajo, la ciberseguridad no ha sido integrada en las consideraciones de la agenda MPS. Ya es hora de asegurarnos que el marco MPS sea apto para abordar los nuevos y emergentes problemas de seguridad, tales como las ciberamenazas y sus implicaciones sobre el género.

Hay múltiples vías para acercar estas áreas de políticas. A nivel nacional, regional y multilateral, por un lado, es importante integrar las consideraciones de género en las políticas de ciberseguridad y, por el otro, incluir la ciberseguridad en las políticas y los planes de acción sobre MPS. En concreto, este trabajo ha delineados seis áreas claves para hacerlo y promover la igualdad de género en el ciberespacio.

- **Participación de las mujeres en las negociaciones de ciberseguridad**

Las mujeres siguen estando subrepresentadas en las negociaciones de ciberseguridad y se necesita más investigación para entender las barreras específicas que están evitando su participación plena, equitativa y satisfactoria. Asimismo, debe continuarse tomando acciones para apoyar la intervención diversa de las mujeres, tales como el programa de becas Women in Cyber Fellowship. Deben complementarse los esfuerzos para aumentar la participación de las mujeres mediante la incorporación activa de las perspectivas de género en las políticas y los programas.

- **Ciberviolencia contra las mujeres y niñas**

Las mujeres de todos los tipos, desde las políticas hasta las defensoras de los derechos humanos y usuarias particulares, enfrentan acoso y amenazas en línea. Para atacar este problema, es importante aumentar la conciencia sobre lo que es la ciberviolencia por medio de campañas públicas. También es necesario asegurarse de que los sistemas legales nacionales estén equipados para prevenir y también procesar casos de ciberviolencia promulgando legislación que penalice los actos de ciberacoso y hostigamiento virtual y capacitando a los sistemas de justicia y policía.

- **Hostigamiento virtual y participación de las mujeres en procesos políticos**

Es crucial garantizar que las mujeres y niñas tengan acceso a las TIC y que puedan usar el espacio digital para su participación cívica. Se requiere más análisis e investigación sobre cómo tales comportamientos en el ciberespacio impactan la participación significativa de las mujeres en la política con el fin de identificar maneras de abordar algunas de estas amenazas.

- **Género y radicalización en línea**

Se necesita más investigación sensible al género y examinar los diferentes factores que influyen en la radicalización de hombres y mujeres, su reclutamiento y su accionar en estos entornos. Se requiere investigación sensible al género sobre los factores que influyen en la radicalización en los entornos digitales. Se necesita un diálogo multiparticipativo que incluya a las empresas de plataformas tecnológicas y de redes sociales para encontrar maneras eficaces de restringir la diseminación de contenido terrorista y la desinformación en línea.

- **Impactos de los ciberincidentes en cuanto al género**

Se requieren más datos desagregados por género y más investigación para entender y abordar el rango de impactos diferenciados de los incidentes de ciberseguridad y los ataques sobre los civiles. Los Estados también deberían procurar incorporar una perspectiva de género en el desarrollo de sus políticas orientadas hacia la protección de infraestructura crítica, incluyendo el cómo enmarcan y definen lo que es una

'infraestructura crítica' y la prioridad asignada a diferentes tipos de incidentes.

- **Sesgos de género en las tecnologías digitales**

Garantizar la diversidad en las fuerzas laborales dedicadas a la informática y la IA y sus procesos es una manera de abordar los sesgos en las tecnologías digitales. Además, es importante integrar perspectivas de género en el desarrollo de las iniciativas de desarrollo de capacidades, materiales y programas de capacitación en informática e IA.

Llevar estas consideraciones a primer plano en la agenda MPS producirá la muy necesaria 'actualización del sistema' y asegurará que la comunidad internacional esté equipada para lidiar con los desafíos de la seguridad internacional del siglo veintiuno y sus implicaciones en cuanto al género.

5. Recomendaciones específicas

La agenda MPS ofrece un marco importante para conceptualizar la 'ciberseguridad' y fortalecer las consideraciones de género en la ciberseguridad. Aprovechando estas lecciones, este trabajo ofrece las recomendaciones siguientes a los Estados, las Naciones Unidas y las organizaciones de la sociedad civil para que las tomen en cuenta como parte de su intervención en los procesos de las Naciones Unidas.

Recomendaciones para los Estados y la Asamblea General

- Integrar las consideraciones de género en las declaraciones nacionales y negociaciones multilaterales sobre las TIC y la ciberseguridad.
- Presentar declaraciones y proponer lenguaje en las resoluciones de la Primera Comisión sobre los desarrollos en el campo de las TIC en el contexto de la seguridad internacional y que el siguiente GTCA:
    - reconozca que el diseño y uso de las TIC puede afectar a hombres, mujeres y otros grupos marginalizados de manera diferente y que las consideraciones de género deben ser aplicadas para reconocer el impacto de las TIC en la paz y la seguridad internacionales;
    - inste a los Estados a continuar sus esfuerzos constantes para aumentar la participación significativa de las mujeres en organizaciones y procesos intergubernamentales que analizan las TIC;
    - reconozca el importante rol de la sociedad civil en las discusiones y negociaciones sobre las TIC en el contexto de la paz y seguridad internacionales y
    - motive a los Estados a integrar las consideraciones de género en el desarrollo de las políticas nacionales de ciberseguridad.
- Reconocer los impactos diferenciados en cuanto al género de las actividades de ciberseguridad en sus declaraciones, resoluciones e informes, incluidas las

resoluciones sobre las mujeres y el desarme en la Primera Comisión. Como reconocimiento a la aplicabilidad de los marcos de derecho internacional a las actividades de ciberseguridad, los Estados podrían hacer referencia específicamente a las obligaciones con respecto a la legislación internacional sobre derechos humanos, particularmente los derechos de las mujeres.

Recomendaciones para los Estados en el Consejo de Seguridad y sus órganos subsidiarios

- Convocar a una reunión con arreglo a la fórmula Arria que se enfoque en el análisis de los vínculos entre la ciberseguridad y las mujeres, la paz y la seguridad.
- Establecer la 'ciberseguridad' como un tema de un próximo debate abierto dentro del punto en la agenda sobre 'mujeres y paz y seguridad' en el Consejo.
- Asegurarse de que las declaraciones presentadas en los debates abiertos sobre MPS reconozcan las oportunidades y amenazas que presentan las TIC y el ciberespacio para la participación y protección de las mujeres y la prevención de conflictos, y reconocer la necesidad de que las perspectivas de género sean integradas en los esfuerzos para fortalecer la ciberseguridad.
- Solicitar que el informe anual de la Secretaría General sobre MPS aborde la ciberseguridad incluyendo los aspectos basados en género y los impactos de los ciberincidentes.
- Utilizar el Grupo Informal de Personas Expertas sobre MPS en el Consejo de Seguridad para hacer preguntas sobre las dimensiones en cuanto al género o el impacto en las mujeres cuando hay ciberincidentes en las situaciones de los países que se están discutiendo.

Recomendaciones para los Estados sobre las políticas nacionales y regionales

- Garantizar que las políticas y actividades nacionales de ciberseguridad de los gobiernos incorporen diversas perspectivas de género en su desarrollo e implementación a todos los niveles del gobierno.
- Integrar las perspectivas de género en el desarrollo de iniciativas, materiales y programas de capacitación para el desarrollo de capacidades informáticas.

- Asegurarse de que los diálogos multiparticipativos que involucren los Estados, la sociedad civil y las empresas de plataformas tecnológicas y de redes sociales consideren la dinámica de género cuando proponen soluciones para restringir la diseminación de contenido terrorista y desinformación en línea.
- Incorporar las diferentes dimensiones de la ciberseguridad en el desarrollo y la revisión de los planes de acción nacionales sobre MPS (incluidos los desarrollados a nivel regional y local).
- Encargar investigaciones y análisis que:
  - recopilen datos desagregados por género y examinen los impactos de los ciberincidentes y ataques contra diferentes comunidades;
  - generar una serie de casos de estudio y enfoques con base en las mejores prácticas para que sirvan de guía a los Estados, las organizaciones internacionales y el sector privado, los cuales podrían incluir un análisis de asuntos relacionados con el cómo los entornos digitales afectan la participación política de las mujeres, las dimensiones en cuanto al género de la radicalización en línea, los impactos diferenciados según el género de los ciberincidentes y el papel de los sesgos en las tecnologías digitales y sus impactos potenciales sobre la igualdad de género y la paz y seguridad internacionales e
  - identificar las barreras para la participación de las mujeres en los procesos multilaterales y multiparticipativos sobre ciberseguridad.

Anexo – Entrevistas y Metodología

Este informe se basó principalmente en una investigación documental de los documentos de las Naciones Unidas, las declaraciones de los Estados y la sociedad civil, informes de investigaciones y trabajos académicos. Esta investigación se complementó con entrevistas a personas diplomáticas y miembros del GEG de Australia, Canadá, Kenia, Malasia y los Países Bajos.

Se usaron los siguientes términos (en inglés) para analizar las 10 resoluciones sobre MPS y todos los debates abiertos del Consejo de Seguridad sobre MPS. Las justificaciones del porqué se escogieron ciertos términos se incluyen a continuación.

'Computer'	Se incluyó para captar cualquier discusión sobre dispositivos mediante los cuales ocurre una interacción en el dominio cibernético.
'Cyber'	Se incluyó pues la frase directamente enmarca este trabajo.
'Information'	Se incluyó para captar referencias a 'tecnología(s) de la información y las comunicaciones'
'Internet'	Se incluyó como una referencia común a los espacios digitales.
'Online'	Se incluyó como una referencia común a los espacios digitales.
'Phone'	Se incluyó para captar cualquier discusión en los primeros años de MPS de las entonces emergentes tecnologías como SMS y redes de teléfonos móviles.
'Technologies'	Se incluyó pues la frase directamente enmarca este trabajo.
'Technology'	Se incluyó pues la frase directamente enmarca este trabajo.

Notas finales

1. Security Council, UN document S/RES/1325, 31 October 2000, https://undocs.org/S/RES/1325(2000).

2. Henri Myrttinen, "Connecting the Dots: Arms Control, Disarmament and the Women Peace and Security Agenda", UNIDIR, 2020, https://unidir.org/sites/default/files/2020-12/Connecting%20the%20Dots_0.pdf.

3. Al momento de redactar este trabajo, estas resoluciones eran las siguientes: 1820 (2009), 1888 (2009), 1889 (2010), 1960 (2011), 2106 (2013), 2122 (2013), 2242 (2015), 2467 (2019) y 2493 (2019).

4. General Assembly, UN document A/AC.290/2021/CRP.3, 10 March 2021, para. 37, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf

5. Katharine Millar, James Shires, and Tatiana Tropina, "Gender Approaches to Cybersecurity: Design, Defence and Response", UNIDIR, 2021, https://doi.org/10.37559/GEN/21/01.

6. Julia Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity", St Antony's International Review vol. 15, no. 1, 2019, https://ssrn.com/abstract=3429851.

7. Para enmarcar estos conceptos y la necesidad de una mayor empatía y sinergia sobre estos temas entre los ciber profesionales, vea Alex Stamos, "Tech's Adversaries vs Enemies", Medium, 13 January 2020, https://medium.com/@alexstamos/techs-adversaries-vs-enemies-a5ca09e09aca.

8. Security Council Report, "In Hindsight: The Security Council and Cyber Threats", 23 December 2019, https://www.securitycouncilreport.org/monthly-forecast/2020-01/the-security-council-and-cyber-threats.php.

9. Debido a las limitaciones de este trabajo, la discusión se enfocará principalmente en las experiencias de mujeres, con algunas consideraciones limitadas a las experiencias de otras identidades de género.

10. UN-Women, "Women, Peace & (Cyber) Security in Asia and the Pacific", 2020, p. 1, https://asiapacific.unwomen.org/en/digital-library/publications/2020/06/action-brief-women-peace-and-cyber-security-in-asia-and-the-pacific.

11. UNIDIR, "The Weaponization of Increasingly Autonomous Technologies: Artificial Intelligence", UNIDIR

Resources, no. 8, 2018, p. 2, https://www.unidir.org/files/publications/pdfs/the-weaponization-of-increasingly-autonomous-technologies-artificial-intelligence-en-700.pdf.

12. Camino Kavanagh, "The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century", UNIDIR, 2017, p. 7, https://www.unidir.org/files/publications/pdfs/the-united-nations-cyberspace-and-international-peace-and-security-en-691.pdf.

13. UNIDIR, "Gender Perspectives", https://unidir.org/gender-perspective.

14. Renata Hessmann Dalaqua, Kjølv Egeland, and Torbjørn Graff Hugo, "Still Behind the Curve: Gender Balance in Arms Control, Non-Proliferation and Disarmament Diplomacy", UNIDIR, p. 10, https://doi.org/10.37559/WMD/19/gen2.

15. Security Council, UN document S/RES/1325, 31 October 2000, https://undocs.org/S/RES/1325(2000).

16. Al momento de redactar este trabajo, estas resoluciones eran las siguientes: 1820 (2008), 1888 (2009), 1889 (2009), 1960 (2010), 2106 (2013), 2122 (2013), 2242 (2015), 2467 (2019), and 2493 (2019).

17. El Consejo de Derechos Humanos adoptó su primera resolución sobre MPS en el 2020; vea UN Document A/HRC/RES/45/28. Vea también Sara E. Davies and Jacqui True (eds), The Oxford Handbook of Women, Peace and Security, 2019.

18. Antes del 2019, todas las resoluciones sobre MPS se habían adoptado unánimemente, aunque durante los procesos de negociación se expresaron algunas diferencias. En abril del 2019, la resolución 2467 no fue adoptada unánimemente debido a la abstención de China y la Federación Rusa; vea Security Council Report, "In Hindsight: Negotiations on Resolution 2467 on Sexual Violence in Conflict", 2 May 2009, https://www.securitycouncilreport.org/whatsinblue/2019/05/in-hindsight-negotiations-on-resolution-2467-on-sexual-violence-in-conflict.php.

19. Estas instituciones tienden a enfocarse en los llamados temas de seguridad 'duros' o 'tradicionales' que se enfocan en las conductas entre Estados en vez de en las preocupaciones de seguridad 'privadas' o 'locales', tales como la violencia basada en género. Vea Phoebe Donnelly, 'Sustaining Feminist Curiosity for the Future of Women, Peace and Security: Q&A with Cynthia Enloe', IPI Global Observatory, 6 October 2020, https://theglobalobservatory.org/2020/10/sustaining-feminist-curiosity-for-future-of-wps-qa-with-cynthia-enloe/; y Julia Slupska, "Safe at Home: Towards a Feminist Critique of Cybersecurity", St Antony's International Review vol. 15, no. 1, 2019, https://ssrn.com/abstract=3429851

20. Para valorar las consideraciones sobre las TIC y el ciberespacio por parte del Consejo de Seguridad en el contexto de MPS, se revisaron y analizaron todos los debates abiertos y las resoluciones sobre MPS desde el 2000 en busca de vínculos con terminología relacionada con 'ciber', 'tecnología', 'en línea' e 'Internet' entre otros términos relacionados; vea el Anexo.

21. Parece que el primer vínculo lo hizo un representante de Bangladesh en el 2008, quien mencionó el potencial de las herramientas de las TIC para aumentar la conciencia del público sobre 'las fortalezas de las mujeres para promover la paz y la seguridad alrededor del mundo'; ver Security Council, UN document S/PV.6005 (Resumption 1), 29 October 2008, p. 10, https://undocs.org/en/S/PV.6005(Resumption1).

22. Vea, por ejemplo, la declaración de Bangladesh en el debate del 2008 sobre MPS (https://undocs.org/en/S/PV.6005); la declaración de Australia del 28 de octubre del 2011 (https://undocs.org/S/PV.6642, p. 33) y la declaración de los Países Bajos del 30 de noviembre del 2012 (https://undocs.org/en/S/PV.6877, p. 56).

23. Vea, por ejemplo, la declaración de los Estados Unidos de América del 18 de octubre del 2013 (https://undocs.org/S/PV.7044, p. 12).

24. Vea, por ejemplo, la declaración de Bélgica del 13 de octubre del 2015 (https://undocs.org/en/S/PV.7533, p. 78); la declaración de Francia del 28 de marzo de 2016 (https://undocs.org/S/PV.7658, p. 26); la declaración de los Emiratos Árabes Unidos (https://undocs.org/S/PV.7704, p. 46) y la declaración de la Unión Europea del 2 de junio del 2016 (https://undocs.org/S/PV.7704, p. 37). Lituania indicó en el debate del 25 de octubre del 2016 que las mujeres periodistas estaban sujetas a troleo y ataques en línea (https://undocs.org/S/PV.7793, p. 89).

25. Vea la declaración de Kenia en el debate del Consejo de Seguridad del 27 de octubre de 2017 (https://undocs.org/S/PV.8079, p. 70).

26. El Grupo Informal de Expertos fue establecido mediante la resolución 2422 para orientar mejor y guiar el trabajo del Consejo sobre MPS. Las discusiones se llevan a cabo entre expertos de países específicos y expertos en MPS de los Estados miembros del Consejo sobre una variedad de situaciones específicas a esos países durante todo el año.

27. Security Council, UN document S/2020/439, 28 May 2020, p. 5, https://undocs.org/S/2020/439.

28. Temas similares se encontraron en el Estudio Global sobre la resolución 1325, que incluyó dos recomendaciones sobre cómo los Estados Miembro y la sociedad civil podrían garantizar mejor el uso positivo de la tecnología para asegurar la prevención y protección durante conflictos y para cerrar 'la brecha

digital de género'; vea UN-Women, Preventing Conflict, Transforming Justice, Securing the Peace: A Global Study on the Implementation of United Nations Security Council Resolution 1325, 2015, p. 407, https://reliefweb.int/sites/reliefweb.int/files/resources/UNW-GLOBAL-STUDY-1325-2015.pdf.

29. Vea, por ejemplo, Security Council, UN document S/2015/203, 23 March 2015, p. 25, https://undocs.org/en/S/2015/203.

30. Security Council, UN document S/2020/946, 25 September 2020, p. 6, https://undocs.org/en/S/2020/946.

31. Ibid., p. 20.

32. Ibid., p. 18.

33. Estos incluyen referencias a 'amenazas relacionadas con la informática en conflictos (Irlanda 2019), el impacto del 'cibercrimen' (Namibia 2019; Kenia 2020) y las amenazas planteadas por el 'ciberacoso' a las organizaciones de mujeres y las defensoras de los derechos humanos (Países Bajos 2021). Consulte más datos en Women's International League for Peace and Freedom, National Action Plans at a Glance, http://1325naps.peacewomen.org/ y Hamilton, Caitlin and Laura J. Shepherd (2020) WPS National Action Plans: Content Analysis and Data Visualisation, v2. Online, at https://www.wpsnaps.org/. Vea también Myrttinen, Henri. 2020. "Connecting the Dots: Arms Control, Disarmament and the Women Peace and Security Agenda". United Nations Institute for Disarmament Research. https://doi.org/10.37559/GEN/20/01

34. Republic of Namibia, "Namibia National Action Plan on Women, Peace and Security: Moving United Nations Security Council Resolution 1325 Forward, 2019–2024", 2019, https://www.peacewomen.org/sites/default/files/Namibia%20NAP%20(2019-2024).pdf.

35. Government of Ireland, "Women, Peace and Security: Ireland's Third National Action Plan for the Implementation of UNSCR 1325 and Related Resolutions 2019–2024", 2019, https://dfa.ie/media/dfa/ourrolepolicies/womenpeaceandsecurity/Third-National-Action-Plan.pdf.

36. General Assembly, UN document A/RES/53/70, 4 January 1999, https://undocs.org/A/RES/53/70.

37. Vea también las respuestas de Australia, el Reino Unidos y Suecia (a nombre de la Unión Europea) en General Assembly, UN document A/54/213, 10 August 1999, https://undocs.org/A/54/213 y General Assembly, UN document A/56/164, 3 July 2001, https://undocs.org/a/56/164.

38. Eneken Tikk-Ringas, "Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998–2012", ICT4Peace, 2012, pp. 4–5, https://ict4peace.org/wp-content/uploads/2012/08/Eneken-GEG-2012-Brief.pdf.

39. General Assembly, UN document A/RES/58/32, 18 December 2003, https://undocs.org/A/RES/58/32.

40. General Assembly, UN document A/65/201, 30 July 2010, https://undocs.org/A/65/201; General Assembly, UN document A/68/98, 24 June 2013, https://undocs.org/A/68/98 y General Assembly, UN document A/70/174, 22 July 2015, https://undocs.org/A/70/174.

41. "Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security", advance copy, 28 May 2021, https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf.

42. General Assembly, UN document A/RES/73/27, 11 December 2018, https://undocs.org/en/A/RES/73/27.

43. Para información detallada sobre las declaraciones nacionales que resaltan la importancia de incorporar el género en el proceso del GTCA, vea Cyber Peace & Security Monitor, vol. 1, no. 7, 2020, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.7.pdf.

44. Vea "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

45. Security'", https://www.un.org/disarmament/wp-content/uploads/2019/09/canadian-position-paper-oewg-en.pdf.

46. Deborah Brown and Allison Pytlak, "Why Gender Matters in International Cyber Security", Women's International League for Peace and Freedom and the Association for Progressive Communications, 2020, https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf; and Katharine Millar, James Shires, and Tatiana Tropina, "Gender Approaches to Cybersecurity: Design, Defence and Response", UNIDIR, 2021, https://doi.org/10.37559/GEN/21/01.

47. General Assembly, UN document A/AC.290/2021/CRP.2, 10 March 2021, para. 12, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

48. Por ejemplo, la Federación Rusa se opuso a incluir algún lenguaje sobre la participación de las mujeres y las perspectivas de género argumentando que esto no se relacionaba con el mandato del GTCA; vea las enmiendas rusas al borrador inicial del GTCA del 19 de enero de 2021, https://front.un-arm.org/wp-content/uploads/2021/02/RF-GTCA-zero-draft-report-with-the-Russian-amendments-ENG.pdf.

49. General Assembly, UN document A/AC.290/2021/CRP.3, 10 March 2021, https://front.un-arm.org/wp-content/uploads/2021/03/Chairs-Summary-A-AC.290-2021-CRP.3-technical-reissue.pdf.

50. Aunque el Resumen de la Presidencia se emitió bajo su propia autoridad, el resumen de las discusiones apareció en todos los borradores discutidos por los Estados y fue comentado y negociado hasta la última sesión del GTCA, cuando se determinó que no se llegaría a un consenso sobre el resumen de las discusiones. En cuanto al contenido del Resumen de la Presidencia, este fue negociado hasta que fue removido del documento resultante, el cual también representa un texto conciliador.

51. De las cinco reuniones realizadas con arreglo a la fórmula Arria que han incluido un enfoque sobre temas relacionados con la informática, tres específicamente se han concentrado en la ciberseguridad. La primera fue en noviembre de 2016, organizada por España y Senegal, sobre el tema 'La ciberseguridad y la paz y seguridad internacionales'. En mayo del 2020, Estonia auspició la segunda reunión con arreglo a la fórmula Arria sobre temas cibernéticos titulada 'Ciberestabilidad, prevención del conflicto y desarrollo de capacidades', y en agosto del 2020 Indonesia (en cooperación con Bélgica, Estonia, Vietnam y el CICR) coordinó una reunión con arreglo a la fórmula Arria sobre 'Ciberataques contra la infraestructura crítica'. Vea Security Council Report, "Arria-formula Meeting on Cyber-Attacks against Critical Infrastructure", 25 August 2020, https://www.whatsinblue.org/2020/08/arria-formula-meeting-on-cyber-attacks-against-critical-infrastructure.php.

52. Vea las declaraciones presentadas por Australia en una reunión con arreglo a la fórmula Arria sobre 'Ciberestabilidad, prevención del conflicto y desarrollo de capacidades' organizada virtualmente el 22 de mayo del 2020, https://vm.ee/sites/default/files/Estonia_for_UN/unsc_-_cyber_arria_22_may_2020_-_australian_statement_002.pdf y por Canadá, https://vm.ee/sites/default/files/Estonia_for_UN/canada-cyber_statement.pdf.

53. Vea la declaración de Ecuador en una reunión con arreglo a la fórmula Arria sobre 'Ciberestabilidad, prevención del conflicto y desarrollo de capacidades' realizada virtualmente del 22 de mayo de 2020; consulte https://vm.ee/sites/default/files/Estonia_for_UN/ecuador_security_council_cyber_stability.pdf

54. Vea la declaración presentada por Irlanda en una reunión con arreglo a la fórmula Arria sobre 'Ciberestabilidad, prevención del conflicto y desarrollo de capacidades' realizada virtualmente del 22 de mayo de 2020, https://vm.ee/sites/default/files/Estonia_for_UN/200521_remarks_arria_meeting_on_cyber_final_written.pdf y por Italia, https://vm.ee/sites/default/files/Estonia_for_UN/riunione_del_cds_in_formato_arria.pdf.

55. Vea la declaración de Italia, ibid., p. 2.

56. Declaración de Canadá en una reunión con arreglo a la fórmula Arria del Consejo de Seguridad sobre los ciberataques contra la infraestructura crítica del 26 de agosto de 2020, https://www.youtube.com/watch?v=CbBchZEG5D8 a las 2:05:20.

57. Declaración de Izumi Nakamitsu, Alta Representante para Asuntos de Desarme, debate abierto del Consejo de Seguridad sobre el 'Mantenimiento de la paz y seguridad internacionales en el ciberespacio' del 29 de junio de 2021, https://un.mfa.ee/wp-content/uploads/sites/57/2021/06/Nakamitsu-29-June.pdf.

58. Cyber Peace & Security Monitor, vol. 1, no. 7, 2020, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.7.pdf.

59. Consulte en el Anexo las generalidades de las entrevistas.

60. Renata Hessmann Dalaqua, Kjølv Egeland, and Torbjørn Graff Hugo, "Still Behind the Curve: Gender Balance in Arms Control, Non-Proliferation and Disarmament Diplomacy", UNIDIR, p. 10, https://doi.org/10.37559/WMD/19/gen2.

61. Ibid.

62. UNIDIR, "Gender in Cyber Diplomacy", 2019, https://unidir.org/sites/default/files/2019-12/Gender%20in%20Cyber%20Diplomacy_Factsheet.pdf.

63. Ibid.

64. Australian Department of Foreign Affairs and Trade, "Women in International Security and Cyberspace Fellowship", press release, 2020, https://www.dfat.gov.au/sites/default/files/wic-fellowship-press-release.pdf.

65. Ibid.

66. Allison Pytlak, "A New 'Women in Cyber' Fellowship has a Big Impact on the GTCA", in Cyber Peace & Security Monitor, vol. 1, no. 7, 2020, p. 15, https://reachingcriticalwill.org/images/documents/Disarmament-fora/other/icts/monitor/CyberMonitor1.7.pdf.

67. General Assembly, UN document A/AC.290/2021/CRP.2, 10 March 2021, para. 12, https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf.

68. UNIDIR, "Gender in Cyber Diplomacy", 2019, https://unidir.org/sites/default/files/2019-12/Gender%20in%20Cyber%20Diplomacy_Factsheet.pdf.

69. UN-Women, "Women, Peace & (Cyber) Security in Asia and the Pacific", 2020, p. 3, https://asiapacific.unwomen.org/en/digital-library/publications/2020/06/action-brief-women-peace-and-cyber-security-in-asia-and-the-pacific.

70. Security Council, UN document S/2020/946, 25 September 2020, p. 18, https://undocs.org/en/S/2020/946.

71. Para una perspectiva similar, vea Sahana Dharmapuri and Jolynn Shoemaker, "Women, Peace and Security and the Digital Ecosystem", Our Secure Future, 2021, https://www.oursecurefuture.org/sites/default/files/WPS%20Digital%20Ecosystem.pdf.

72. Estas pueden verse como ejemplos de 'violencia semiótica'; vea Alexis Henshaw, "Bringing Women, Peace and Security Online: Mainstreaming Gender in Responses to Online Extremism", Global Network on Extremism and Technology, 2021, https://gnet-research.org/wp-content/uploads/2021/03/GNET-Report-Women-Peace-And-Security.pdf.

73. Henri Myrttinen, "Connecting the Dots: Arms Control, Disarmament and the Women Peace and Security Agenda", UNIDIR, 2020, https://unidir.org/sites/default/files/2020-12/Connecting%20the%20Dots_0.pdf.

74. UN-Women, "Women, Peace & (Cyber) Security in Asia and the Pacific", 2020, https://asiapacific.unwomen.org/en/digital-library/publications/2020/06/action-brief-women-peace-and-cyber-security-in-asia-and-the-pacific.

75. Ibid.

76. Linda Baker, Marcie Campbell and Elsa Barreto, "Understanding Technology-Related Violence Against Women: Types of Violence and Women's Experiences", Learning Network Brief 6, Centre for Research and Education on Violence Against Women and Children, Western University, 2013, http://www.vawlearningnetwork.ca/our-work/briefs/brief-06.html.

77. Aquellos Estados que no han experimentado conflictos recientemente o que están caracterizados como 'desarrollados' a menudo cuentan con PAN que 'ven hacia afuera', en vez de atender los problemas de preocupaciones locales (tales como la condición de las poblaciones de refugiados, indígenas y desplazadas). No obstante, esto está empezando a cambiar; vea Security Council, UN document S/2020/946, 25 September 2020, p. 26, https://undocs.org/en/S/2020/946.

78. Consulte los indicadores del 2020 recopilados por la Unión Internacional de Telecomunicaciones en https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ITU_regional_global_Key_ICT_indicator_aggregates_Nov_2020.xlsx.

79. UN-Women, Preventing Conflict, Transforming Justice, Securing the Peace: A Global Study on the Implementation of United Nations Security Council resolution 1325, 2015, p. 202, https://reliefweb.int/sites/reliefweb.int/files/resources/UNW-GLOBAL-STUDY-1325-2015.pdf.

80. Security Council, UN document S/2020/946, 25 September 2020, p. 6, https://undocs.org/en/S/2020/946.

81. Security Council, UN document S/2019/800, 9 October 2019, https://undocs.org/en/S/2019/800; vea también General Assembly, UN document A/74/821, 29 May 2020, p. 8, https://undocs.org/A/74/821.

82. Security Council, UN document S/2020/946, 25 September 2020, p. 20, https://undocs.org/en/S/2020/946.

83. Lucina Di Meco and Kristina Wilfore, "Gendered Disinformation is a National Security Problem", Tech Stream, 8 March 2021, https://www.brookings.edu/techstream/gendered-disinformation-is-a-national-security-problem/.

84. Hannah Smith and Katherine Mansted, "Weaponised Deep Fakes. National Security and Democracy", policy brief, Report No. 28, Australian Strategic Policy Institute, 2020, p. 5, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-04/Weaponised%20deep%20fakes.pdf.

85. Ian Sample, "What are Deepfakes—and How Can You Spot Them?", The Guardian, 13 January 2020, https://www.theguardian.com/technology/2020/jan/13/what-are-deepfakes-and-how-can-you-spot-them. Oliver Ward, "Sex and Deepfakes: Sexualised Misinformation will Hamper Future Female Democratic Participation", ASEAN Today, 21 November 2019, https://www.aseantoday.com/2019/11/sex-and-deepfakes-sexualised-misinformation-will-hamper-future-female-democratic-participation/; "Altered Image: Burma's Aung San Suu Kyi 'in Fake Headscarf'", BBC News, 9 June 2014, https://www.bbc.com/news/blogs-news-from-elsewhere-27740282 y Raphael Satter, "Deepfake Used to Attack Activist Couple Shows New Disinformation Frontier", Reuters, 15 July 2020, https://www.reuters.com/article/us-cyber-deepfake-activist/deepfake-used-to-attack-activist-couple-shows-new-disinformation-frontier-idUSKCN24G15E.

86. Naseem Tarawnah, "Sextortion, Harassment, and Deepfakes: How Digital Weapons are Being Used to Silence Women", IFEX, 5 March 2020, https://ifex.org/sextortion-harassment-and-deepfakes-how-digital-weapons-are-being-used-to-silence-women/; "Deepfake Poses a Threat to Human Rights Defenders in the Middle East", Gulf Centre for Human Rights, 14 October 2019, https://www.gc4hr.org/news/view/2227.

87. Agnes E. Venema, "Deepfakes as a Security Issue: Why Gender Matters", Women in International Security, 4 November 2020, https://www.wiisglobal.org/deepfakes-as-a-security-issue-why-gender-matters/

88. Security Council, UN document S/2020/946, 25 September 2020, p. 24, https://undocs.org/en/S/2020/946.

89. Mehmet Ümit Necef, "'If Men Were Men, then Women Would be Women': ISIL's Construction of Masculinity and Femininity", Center for Modern Middle East and Muslim Studies, University of Southern Denmark, 2016, p. 4, https://www.sdu.dk/-/media/files/om_sdu/centre/c_mellemoest/videncenter/artikler/2016/necef+article+may+16.pdf.

90. Chantal de Jonge Oudraat and Michael E. Brown, "Women, Gender, and Terrorism: The Missing Links", policy brief, Women in International Security, 1 August 2016, pp. 3 and 6, https://wiisglobal.org/wp-content/uploads/2014/02/WIIS-Policy-Brief_Women-Gender-and-Terrorism-The-Missing-Links.pdf.

91. Elizabeth Pearson, "Online as the New Frontline: Affect, Gender, and ISIS-Take-Down on Social Media", Studies in Conflict & Terrorism, vol. 41, no. 11, 2018, https://doi.org/10.1080/1057610X.2017.1352280.

92. Ibid.

93. Sanchez, Sergio E., "The Internet and the Radicalization of Muslim Women", paper presented at the annual meeting of the Western Political Science Association, Seattle, 17 April 2014, p. 8, http://www.wpsanet.org/papers/docs/The%20Internet%20and%20the%20Radicalization%20of%20Muslim%20Women.pdf.

94. Maura Conway, Ryan Scrivens and Logan Macnair, "Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends", policy brief, International Centre for Counter-Terrorism, October 2019, p. 2, https://icct.nl/wp-content/uploads/2019/11/Right-Wing-Extremists-Persistent-Online-Presence.pdf.Counter-Terrorism Committee Executive Directorate, "Member States Concerned by the Growing and Increasingly Transnational Threat of Extreme Right-Wing Terrorism", CTED Trends Alert, April 2020, p. 5, https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/cted_trends_alert_extreme_right-wing_terrorism.pdf.

95. Manoel Horta Ribeiro et al. 2021. "The Evolution of the Manosphere Across the Web", Proceedings of the Fifteenth International AAAI Conference on Web and Social Media, 8¬–10 June 2021, p. 205, https://ojs.aaai.org/index.php/ICWSM/article/view/18053.

96. El Foro Global en Internet contra el Terrorismo es un ejemplo de una plataforma multiparticipativa.

97. Como un ejemplo, puede mencionarse que Christchurch Call — por un compromiso de los gobiernos y las empresas de tecnología de eliminar el contenido extremista violento y terrorista — no hace ninguna referencia a cuestiones de género.

98. Deborah Brown and Allison Pytlak, "Why Gender Matters in International Cyber Security", Women's

99. International League for Peace and Freedom and the Association for Progressive Communications, 2020, p. 6, https://www.apc.org/sites/default/files/Gender_Matters_Report_Web_A4.pdf.

100. Ibid.

101. Ibid, p. 12.

102. Katharine Millar, James Shires, and Tatiana Tropina, "Gender Approaches to Cybersecurity: Design, Defence and Response", UNIDIR, 2021, https://doi.org/10.37559/GEN/21/01.

103. Susan Leavy, "Gender Bias in Artificial Intelligence: The Need for Diversity and Gender Theory in Machine Learning", Proceedings of the First International Workshop on Gender Equality in Software Engineering, Gothenburg, Sweden, 28 May 2018, https://doi.org/10.1145/3195570.3195580.

104. Katharine Millar, James Shires, and Tatiana Tropina, "Gender Approaches to Cybersecurity: Design, Defence and Response", UNIDIR, 2021, https://doi.org/10.37559/GEN/21/01.

105. Julia Slupska and Leonie M. Tanczer, "Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things", The Emerald International Handbook of Technology-Facilitated Violence and Abuse, https://www.emerald.com/insight/content/doi/10.1108/978-1-83982-848-520211049; Vea también Simon Parkin, et al. 2019, "Usability Analysis of Shared Device Ecosystem Security: Informing Support for Survivors of IoT-Facilitated Tech-Abuse", Proceedings of the New Security Paradigms Workshop, San Carlos, Costa Rica, 23–26 September 2019, https://doi.org/10.1145/3368860.3368861.

106. Los modelos de amenazas basados en género también deberían estar presentes a nivel estatal, tal como en los procesos de acciones de vulnerabilidad. Vea Sven Herpig and Ari Schwartz, "The Future of Vulnerabilities Equities Processes Around the World", Lawfare, 4 January 2019, https://www.lawfareblog.com/future-vulnerabilities-equities-processes-around-world.

107. World Economic Forum, "Assessing Gender Gaps in Artificial Intelligence", 2018, https://reports.weforum.org/global-gender-gap-report-2018/assessing-gender-gaps-in-artificial-intelligence/; ONU Mujeres ha notado que más del 70 por ciento de los profesionales en inteligencia artificial son hombres; vea "Women, Peace & (Cyber) Security in Asia and the Pacific", 2020, p. 3, https://asiapacific.unwomen.org/en/digital-library/publications/2020/06/action-brief-women-peace-and-cyber-security-in-asia-and-the-pacific.

108. Surya Deva, "Addressing the Gender Bias in Artificial Intelligence and Automation", Open Global Rights, 10 April 2020, https://www.openglobalrights.org/addressing-gender-bias-in-artificial-intelligence-and-automation/.

109. Vyacheslav Polonski, "AI is Convicting Criminals and Determining Jail Time, but Is it Fair?", World Economic Forum, 19 November 2018, https://www.weforum.org/agenda/2018/11/algorithms-court-criminals-jail-time-fair/. Vea también UN-Women, "Women, Peace & (Cyber) Security in Asia and the Pacific", 2020, p. 3, https://asiapacific.unwomen.org/en/digital-library/publications/2020/06/action-brief-women-peace-and-cyber-security-in-asia-and-the-pacific; World Bank, World Development Report 2016, 2016, p. 134, http://documents1.worldbank.org/curated/en/896971468194972881/pdf/102725-PUB-Replacement-PUBLIC.pdf.

110. Sarah Shoker, "Making Gender Visible in Digital ICTs and International Security", report commissioned by Global Affairs Canada, 2020, p. 6, https://front.un-arm.org/wp-content/uploads/2020/04/commissioned-research-on-gender-and-cyber-report-by-sarah-shoker.pdf.

ACTUALIZACIÓN DEL SISTEMA: HACIA UNA AGENDA SOBRE MUJERES, PAZ Y CIBERSEGURIDAD

Actualización del sistema por una parte explora la relación entre la agenda Mujeres, Paz y Seguridad (MPS) y, por la otra, la amenazas facilitadas por la informática y la ciberseguridad. El trabajo analiza los vínculos entre los temas prioritarios de MPS – igualdad de género, participación de las mujeres en la seguridad internacional, prevención de la violencia contra las mujeres y su protección, las necesidades diferenciadas por género – y la ciberseguridad internacional. Identifica las áreas prioritarias que deben abordarse para garantizar un ciberespacio inclusivo en cuanto al género que proteja los derechos de las mujeres y niñas.