ICT for peace
FOUNDATION

CYBER SECURITY
POLICY PROCESS
BRIEF

¿UN PAPEL PARA LA SOCIEDAD CIVIL?

TIC, NORMAS Y MEDIDAS DE CONSTRUCCIÓN DE CONFIANZA EN EL CONTEXTO DE LA SEGURIDAD INTERNACIONAL

Camino Kavanagh y Daniel Stauffacher

GINEBRA 2015
ICT4Peace Foundation

ICT4Peace Publishing, Ginebra.

Copias disponibles en www.ict4peace.org

¿UN PAPEL PARA LA SOCIEDAD CIVIL?

TIC, NORMAS Y MEDIDAS DE CONSTRUCCIÓN DE CONFIANZA EN EL CONTEXTO DE LA SEGURIDAD INTERNACIONAL

Camino Kavanagh y Daniel Stauffacher

ICT for peace FOUNDATION

AGRADECIMIENTOS

Los autores desean agradecer a Ben Basley-Walker (UNIDIR), Gustavo Diniz (Instituto Igarrape), el Dr. Roger Hurwitz (CSAIL-MIT), So Jeong KIM (National Security Research Institute of ETRI), Mihoko Matusbara (Hitachi Systems SSRC/ Pacific Forum CSIS), Sanjana Hattotuwa (ICT4Peace), Ben Hiller (OSCE), Prof. Duncan Hollis (Temple University), Tim Maurer (New America Foundation), Emb. (r) Paul Meyer (Simon Fraser University), Chris Parsons (Citizen Lab, University of Toronto), Robert Parker y An Vranckx (SaferWorld), el Dr. Tim Stevens (King's College London), el Dr. Eneken Tikk-Ringas (IISS) y un sinnúmero de otros colegas por los comentarios profundos y sugerencias que ayudaron a darle forma a este documento.

Finalmente, también deseamos agradecer al Programa de Seguridad Cibernética de la Secretaría de la OEA/CICTE por la traducción al español, y en especial a Belisario Contreras por su apoyo durante todo el proceso.

INTRODUCCIÓN

Como se ha señalado en publicaciones anteriores de ICT4Peace, en los últimos cinco años, los Estados han participado cada vez más en discusiones de políticas sobre normas, medidas de construcción de confianza y capacidad encaminadas a la reducción del riesgo y la construcción de confianza entre los Estados con respecto a los usos de las tecnologías de información y comunicaciones (TIC). En 2013, un Grupo de Expertos Gubernamentales de las Naciones Unidas (GEG) y la Organización para la Seguridad y la Cooperación en Europa (OSCE) llegaron a un acuerdo inicial sobre la naturaleza de algunas de estas normas y medidas de construcción de confianza y capacidad (CBM). No obstante, los debates de fondo se encuentran en una etapa temprana. Los gobiernos han reconocido la necesidad de construir confianza y profundizar su compromiso con otros grupos, incluyendo organizaciones de la sociedad civil, a medida que avanzan para formular nuevas normas y reglas en este área. Como veremos, la participación de la sociedad civil en materia de gobernanza y seguridad internacional no es nueva y hay decenas de ejemplos de áreas en las que los Estados se han adaptado a tal compromiso. La seguridad cibernética no debe ser una excepción. Además, es un área que, por su propia naturaleza y la amplia gama de intereses normativos involucrados, exige una participación más dinámica de la sociedad civil que la que se experimenta en otras áreas. Si se aborda eficaz y coherentemente, sostenemos que tal participación puede generarle una mayor legitimidad y sostenibilidad a procesos de medidas de construcción de confianza y normas multilaterales continuas en relación con seguridad internacional y el uso estatal de las TIC. También puede ayudar a asegurar que sean atendidos unos asuntos normativos más extensos, y que se asegure la experiencia técnica adecuada cuando se estén buscando soluciones. En conjunto, este último puede ayudar a construir confianza entre los Estados y entre los Estados y la sociedad.

Hemos dividido este documento en tres secciones: la primera ofrece una breve visión general del contexto actual; el segundo explica por qué la sociedad civil es importante en la promoción de las normas y medidas de construcción de confianza con respecto al uso de las TIC en el contexto de la seguridad internacional y regional; y la tercera propone unas sugerencias para la participación de la sociedad civil en tres categorías: i) la participación efectiva; ii) el fomento de la transparencia y la rendición de cuentas; y iii) la profundización del conocimiento.[1]

El documento está dirigido a las organizaciones de la sociedad civil, los gobiernos nacionales, organizaciones internacionales y regionales y otros actores involucrados con las TIC y su impacto en la seguridad internacional y regional. A los efectos de

[1] Este documento se basa en una presentación hecha por el Emb. (r) Daniel Stauffacher sobre Medidas de Creación de Confianza y Normas de Seguridad Cibernética y el futuro de la Gobernanza de Internet organizada por el Centro de Excelencia para la Seguridad Nacional (CENS) de la Escuela S. Rajaratnam de Estudios Internacionales (LER), Singapur, 03-04 de julio de 2014.

este documento, definimos sociedad civil como una esfera social separada tanto del Estado como del mercado y conformada por organizaciones no estatales, sin fines de lucro, o de voluntariado. Las organizaciones de la sociedad civil pueden unir a la gente en diferentes niveles (local, nacional, regional e internacional) para avanzar en objetivos e intereses compartidos, trabajando en una serie de áreas temáticas. Llevan a cabo una amplia gama de funciones, incluyendo la investigación orientada a las políticas, promoción y creación de redes. Pueden realizar funciones de vigilancia/monitoreo y con frecuencia coordinan o representan a otros grupos y organizaciones. En el mundo de la seguridad cibernética/Internet, las organizaciones de la sociedad civil a menudo trabajan en áreas de interés específicas, muchas de naturaleza técnicas o funcionales y vinculadas al mantenimiento de la Internet. Otros abogan por ciertos intereses cívicos tales como la privacidad. A menudo, el área de trabajo está proscrita por el contexto nacional. La sociedad civil no incluye el sector privado. Sin embargo, están surgiendo alianzas naturales entre algunas de las organizaciones de la sociedad civil más técnicamente orientadas (por ejemplo, la Internet Society o la IEEE) y algunos proveedores de nivel 1 (es decir, los proveedores que tienen una conexión directa a Internet y las redes que utiliza para entregar servicios de voz y datos) y principales proveedores transnacionales y proveedores de servicios de Internet (ISP).

1. EL CONTEXTO

Sin duda estamos viviendo un momento de cambio importante en el que una serie de acontecimientos han llevado a la pérdida de confianza del público, a una falta de confianza entre gobernantes y gobernados. Los vínculos entre los estados, por un lado, y entre el Estado y ciudadanos por el otro, están siendo desafiados cada vez más por una serie de prácticas estatales, incluyendo usos negativos de las TIC para adelantar objetivos políticos, militares y económicos. Esta situación ha surgido en un momento en que se ha reducido considerablemente la confianza de los ciudadanos en el comportamiento de los actores estatales (y políticos). Evidencia de esta desconfianza se manifestó en las convocatorias de una representación democrática mejorada y un gobierno más eficaz en las regiones al llegar a su fin la primera década del 2000; y ha sido un tanto agravada por las recientes revelaciones de prácticas de supervisión y vigilancia sin control por parte de una serie de gobiernos.

A pesar de la proliferación de predicciones de tragedias por parte de numerosos funcionarios del gobierno en los últimos cinco años, gracias a Dios no ha sucedido una 'ciberguerra' total o un incidente al estilo Armagedón, ni es probable que ocurra en un futuro próximo, no solo desde una perspectiva de teoría estratégica[2],

[2] Véase, por ejemplo, Libicki, Martin, (2014), Why Cyber War Will Not and Should Not Have Its Grand Strategist. *Strategic Studies Quarterly* (Spring 2014); Rid, Thomas (2013), *Cyber War Will Not Take Place*. Oxford University Press; Betz, David (2013), Cyber Power in Strategic Affairs: Neither Unthinkable nor Blessed | Kings of War, *Journal of Strategic Studies*, 35:5, 689-711, DOI: 10.1080/01402390.2012.706970

sino también debido a las asimetrías que subsisten entre los Estados y entre los Estados y los actores no estatales en esta materia. Las TIC, sin embargo, cada vez más son utilizadas por los Estados y sus adversarios para incrementar paulatinamente la ventaja durante los conflictos armados o situaciones de disputa política tensa. De hecho, se han utilizado las TIC y las capacidades cibernéticas ya sea como medio de ataque o como blanco de ataque, por ejemplo:

- En el contexto de conflictos más amplios (Georgia, 2008; y Siria desde el comienzo de la guerra civil).

- Fuera del contexto de un conflicto armado abierto, se ha utilizado el uso directo o manipulación de las TIC para lograr los objetivos políticos y estratégicos (por ejemplo, en Estonia 2007; Irán en 2010, la República de Corea en 2013), supuestamente demostrando, en particular en el caso de Irán (a través de Stuxnet en la Operación Juegos Olímpicos)[3] que la manipulación de las TIC (o más bien, sabotaje impulsado por las TIC) puede tener un impacto importante en la infraestructura crítica de un país.[4]

Estos desarrollos, en particular el creciente interés de los Estados en el desarrollo de lo que se refiere con frecuencia como capacidades cibernéticas ofensivas y defensivas, han tenido lugar en un contexto de importantes cambios en el entorno estratégico global más amplio: el ascenso de China como un poder militar regional y económico mundial y la marcada asertividad en la política internacional y regional por parte de muchos crecientes estados de ingresos medios y la percepción de un alejamiento gradual del poder de Occidente;[5] un recrudecimiento del extremismo y crimen organizado en todas las regiones; la crisis financiera mundial, cuyos efectos siguen resonando en el ámbito nacional, especialmente entre los jóvenes desempleados (y cada vez más conocedores de la tecnología) en las mega-ciudades del mundo; y grietas en el orden internacional de la posguerra fría, entre ellos un rechazo explícito por parte de algunos dirigentes de normas y principios democráticos, en conjunto con un desencanto ciudadano cada vez mayor con el estado de bienestar liberal y la percepción de su inhabilidad de responder. La incertidumbre en el entorno internacional provocada por estos cambios ha exacerbado la sensación de complejidad y desconfianza alrededor de las discusiones sobre "ciberespacio" y los usos de las tecnologías de la información y las comunicaciones (TIC) para la consecución de objetivos políticos, militares o económicos.

El interés de una mayor participación del Estado fue avivado inicialmente por los acontecimientos en Estonia en 2007. Estos eventos inadvertidamente coincidieron

[3] David E. Sanger, *Confront and Conceal*: *Obama's Secret Wars and Surprising Use of American Power*, Broadway Books. (2012). Sin embargo, el impacto real de Stuxnet se ha disputado cada vez más.

[4] Es importante señalar en este sentido que los estados continúan definiendo la infraestructura crítica de manera diferente

[5] Véase *inter alia*, Carothers, T. et al, en 'Is the World Falling Apart?' 14 de agosto de 2014. Dotación Carnegie para la Paz Internacional. Disponible en: http://carnegieendowment.org/2014/08/14/is-world-falling-apart/hkuw

con un período de intensas luchas territoriales en los Estados Unidos sobre la entidad responsable de la defensa cibernética. Luego, entre 2009 y 2012, un número creciente de gobiernos propusieron desarrollar y publicar estrategias nacionales de seguridad cibernética.[6] Unos gobiernos, en particular de tipo autoritario, se centraron en el papel potencialmente desestabilizador de las TIC y los medios de comunicación social como ciudadanos vieron las nuevas oportunidades que prometían para la organización y para expresar su disenso.[7] La Organización de Cooperación de Shanghai (OCS) formalizó estas preocupaciones en un acuerdo regional en el año 2009.[8] Esta atención aumentó y se extendió por las regiones a medida que se percibía que las TIC (quizás exageradamente) habían tenido un papel fundamental en la agitación política en el norte de África y los conflictos más recientes en el Medio Oriente, con algunos gobiernos se dedicaron a cerrar, bloquear el acceso, o filtrar el tráfico de la red en el punto álgido de las crisis. Varios gobiernos de diferentes tipos también comenzaron a utilizar las plataformas sociales como herramientas de propaganda en contra de los ciudadanos alzados en armas, para mantener la lealtad de los partidarios del régimen y propagar una narrativa alternativa sobre el conflicto tanto en el país como en el extranjero.[9]

Estos acontecimientos fueron a su vez seguidos por las revelaciones de que los estados utilizaban malware sofisticado como Stuxnet para alcanzar objetivos de política exterior y se describieron prácticas de supervisión y vigilancia amplias y en gran medida sin control por parte de los organismos de inteligencia de estados tanto democráticos como autoritarios. Lo que ha surgido es que muchas de estas prácticas estaban justificadas por motivos de seguridad nacional. Muchas otras no. Mientras tanto, se percibe que algunas empresas privadas están tomando un papel cada vez más polémico en la defensa contra diferentes usos de las TIC por parte de actores estatales y no estatales, a través de la práctica de la "defensa activa".[10] Si bien los datos reales que rodean estas prácticas es difícil de conseguir, han provocado, no obstante, fuertes reacciones por parte de actores estatales y no estatales, algunos de los cuales se han apresurado a emular en lugar de ayudar a establecer normas y reglas para su uso.[11] Además, muchos Estados menos sofisticados tecnológicamente

---

[6] Cyber Index: International Security Trends and Analysis (2013), CSIS, IPRSP, UNIDIR. Disponible en: http://www.unidir.org/files/publications/pdfs/cyber-index-2013-en-463.pdf

[7] Kavanagh, C (2012), 'The Limits of Dissent in Cyberspace'. Policy Brief prepared for CyberDialogue 2012: What is Stewardship in Cyberspace. Marzo 18-19, 2012, Toronto, Canada. http://www.cyberdialogue.citizenlab.org/wp-content/uploads/2012/2012briefs/brief-1.pdf

[8] Acuerdo SCO sobre Cooperación en Materia de Seguridad de la Información

[9] Clark, M. y Abas A., 'The Hard Realities of Soft Power: Keeping Syrians Safe in a Wired War,' Documento de antecedentes, SecDev, 12 de junio de 2013. Disponible en: http://gallery.mailchimp.com/eb7c0bde6ff78e88f9b0c8662/files/SecDev_wiredconflict_25June2013.pdf?utm_source=Syria+report+distribution+list&utm_campaign=1ae1bd351d-MIGS-1&utm_medium=email&utm_term=0_8b953783f7-1ae1bd351d-52609969

[10] La falta de marcos regulatorios nacionales o normas internacionales y estándares relativos a este último se hace eco de los problemas similares que surgieron con la proliferación de empresas militares privadas en la década de 1990, en la que la externalización de las necesidades militares conducen a una pérdida de control democrático sobre el ejército, lo que plantea desafíos a cuestiones de soberanía, incluyendo a través de la disminución del monopolio del Estado sobre el uso de la fuerza.

[11] Para conocer una discusión sobre las dimensiones legales del debate Hack-Back, consulte Alexei Alexis, 'Debate Brewing Over Whether Companies Should Strike Back at Their Cyber Attackers,' Bloomberg, 19 de abril de 2013. El Comité Permanente de la American Bar Association para el Derecho y Seguridad Nacional también ha desarrollado una línea de trabajo en este área. Véase, por ejemplo: http://www.abajournal.com/news/article/how_far_should_companies_be_allowed_to_go_to_hunt_cy

están aprovechando el creciente mercado, facilitado principalmente por empresas privadas occidentales, de software de detección de intrusos (por ejemplo, FinFisher spyware).[12]

Aprovechando las lagunas normativas y reglamentarias existentes (y los avances tecnológicos que han eliminado muchos obstáculos financieros y prácticos), algunos estados se han apresurado a desarrollar o adquirir estas y otras herramientas y capacidades, para usarlas contra otros estados, como medio para promover sus intereses, y domésticamente para el control político y la represión de los medios de comunicación y la sociedad civil. Esta realidad, que se manifiesta a través de una gama de regímenes políticos, tiene el potencial de socavar aún más la confianza entre los Estados y entre Estados y ciudadanos.[13] En respuesta a estos acontecimientos, se ha iniciado una serie de esfuerzos nacionales e internacionales para gestionar el uso de las TIC y configurar la conducta del Estado en ciberespacio. Sin embargo, los diferentes valores e intereses de la sociedad, problemas de atribución, tecnología en constante evolución, el comportamiento de algunos estados, y el papel desempeñado por ciertas empresas privadas en este campo han planteado barreras para llegar a un consenso.[14] Por ejemplo, a pesar de estar de acuerdo sobre la aplicabilidad al ciberespacio del derecho internacional vigente,[15] los estados aún no han podido definir lo que se constituye en un "ataque cibernético" o un "arma cibernética" en el contexto del derecho internacional humanitario (en especial el debate de los medios frente a los efectos) o en derecho y política internacional en general.[16]

Por otra parte, muchos de los esfuerzos en curso para llegar a un consenso se han topado con dificultades sobre todo porque es difícil (pero no del todo imposible) adaptarse a las TIC en los paradigmas tradicionales de seguridad. Por ejemplo, se han hecho intentos para adaptar las TIC a los marcos tradicionales de control de armas. Este enfoque ha sido complejo, debido en gran parte al número de diferentes actores involucrados en la cadena de suministro de seguridad, lo que probablemente plantearía dificultades en términos de llegar a acuerdos sobre

berattackers/ o http://www.americanbar.org/news/abanews/aba-news-archives/2013/08/_active_cyber_defens.html

[12] Comunicación por correo electrónico entre Duncan Hollis, Vicedecano de Asuntos Académicos y James A. Beasley Profesor de Derecho, Universidad de Temple, 15 de agosto de 2014.

[13] El reciente informe del ACNUDH sobre el derecho a la privacidad en la era digital señala cómo "El Estado ahora tiene una mayor capacidad para llevar a cabo vigilancia simultánea, invasiva, específica y a gran escala que nunca antes", lo que sugiere que estas nuevas capacidades aumentadas han llevado a la infracción del derecho a la privacidad y otros derechos fundamentales. El informe fue el resultado de la resolución de la Asamblea General de la ONU sobre "El derecho a la privacidad en la era digital", aprobada sin votación en el III Comité (Derechos Humanos) y después por la Asamblea General en 2013, y será discutido en las sesiones del Consejo General de Derechos Humanos y la Asamblea general de este año. Véase: Derecho a la privacidad en la era digital: Informe de la Oficina del Alto Comisionado de la ONU para los Derechos Humanos (A/HRC/27/37) del 30 de junio de 2014. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

[14] Hathaway, M. E. (por salir), Connected Choices: How the Internet is Challenging Sovereign Decisions, *American Foreign Policy Interests*.

[15] Informe del Grupo de Expertos Gubernamentales de la ONU sobre los Avances en la Esfera de la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional, junio de 2013.

[16] Comunicación con el UNIDIR, 25 de agosto de 2014.

garantías y certificaciones.[17] No obstante, en diciembre de 2013, los Estados miembros del Acuerdo de Wassenaar anunciaron nuevos controles relacionados con el 'software de detección de intrusos' y los 'sistemas de vigilancia de red IP", que darán lugar a cambios en los regímenes nacionales de control de exportaciones de los estados miembros en los próximos años.[18] Este fue un paso importante, aunque será importante monitorear cómo se traducirán los nuevos controles en la práctica.

Más allá del panorama estratégico tradicional, ya en 1990 se había reconocido el riesgo de una creciente "brecha digital", en la que las TIC podrían reforzar en vez de reducir las desigualdades a nivel internacional como a nivel nacional, en un informe de expertos sobre Nuevas Tecnologías y Seguridad Internacional presentado a la Asamblea general. El informe señaló proféticamente: 'para los países en desarrollo que carecen de medios para adquirir información, el aumento del costo real de la información hace que les sea más difícil mantenerse al día. A algunos de ellos les preocupa profundamente que la revolución de la tecnología de la información los deje atrás como ha hizo la revolución industrial. La seguridad radica en el acceso a la información'.[19] Unos trece años más tarde, la Declaración de principios de Ginebra de la CMSI y el Plan de Acción que lo acompañaba (2003)[20] hicieron énfasis en el papel central de las TIC en muchas áreas de desarrollo económico y social, recomendando que las TIC se aprovechen para transformar la brecha digital en una oportunidad digital para todos. Sin embargo, como se reconoció también, solo pueden alcanzarse el desarrollo económico y la prosperidad si el contexto nacional y regional es estable y pacífico.[21] En todo el mundo, muchas regiones que se encuentran afectadas por conflictos continúan perdiendo oportunidades de desarrollo. El retorno de la inversión en la prevención de conflictos, la mitigación de la violencia y en la construcción de una paz duradera es significativamente mayor que las inversiones que se requieren para reconstruir los países y construir la paz después de los conflictos y la violencia.[22] Y como cada vez se reconoce más, las TIC pueden desempeñar un papel importante en este sentido;

[17] Sin embargo, hay ejemplos de regímenes mixtos de estado, sector privado y sociedad civil en otros ámbitos, por ejemplo en la aviación civil, que podrían considerarse parte de los mecanismos tradicionales de seguridad internacional, y cuyas lecciones valdría la pena estudiar más en detalle. Comunicación por correo electrónico con Roger Hurwitz, investigador científico, MIT-CSAIL 10 de agosto de 2014.

[18] Como lo han señalado por Maurer *et al*, es importante tener en cuenta que el software de intrusión en sí no se controló. En cambio, la redacción de los controles es muy explícito en que solo están sujetos a control los componentes para la generación, manejo, entrega y comunicación con el malware. En otras palabras, "la lista de control se dirige a aquellos que compren software de intrusión y traten de tener a los demás como su objetivo, no a los que están infectados por este."

[19] Informe del Secretario General, Evolución Tecnológica y Científica y su Impacto en la Seguridad Internacional. A/45/568 del 17 de octubre de 1990.

[20] Declaración de Principios y Plan de Acción CMSI, Ginebra 2003 (Documento WSIS-03/GENEVA/DOC/5-E). Disponible en: Documento WSIS-03/GENEVA/DOC/5

[21] Véase el Informe del Grupo de Alto Nivel sobre la Agenda de Desarrollo Post-2015; véase también la pieza blog del Centro de Cooperación Internacional (CIC), 'El papel de la paz y la seguridad en la Agenda de Desarrollo Post-2015: la perspectiva de los Estados de África y los países menos desarrollados', disponible en: http://cic.nyu.edu/blog/global-development/role-peace-and-security-post-2015-agenda-perspective-african-states-and-ldcs

[22] Véase: Banco Mundial. 2011. *World Development Report 2011: Conflict, Security, and Development*. Banco Mundial. © Banco Mundial. https://openknowledge.worldbank.org/handle/10986/4389 Licencia: CC BY 3.0 IGO."

sin embargo, a menos que se sustente el progreso en negociaciones internacionales y regionales, su uso negativo puede eclipsar ese potencial.[23]

2. NORMAS, CBM Y SOCIEDAD CIVIL: ¿POR QUÉ?

Durante las últimas décadas, la mayoría de los gobiernos han aceptado el papel que las normas y las medidas de construcción de confianza (CBM) pueden desempeñar en el fortalecimiento de la confianza entre los Estados y dentro de los Estados. Además, los principios básicos de gobernanza, tales como la participación, la transparencia y rendición de cuentas puede ayudar a construir y profundizar la confianza entre los Estados y entre Estados y ciudadanos.[24] Estos procesos y principios a menudo se superponen y pueden entrar en conflicto (por ejemplo, el equilibrio entre apertura y privacidad; derechos y seguridad); por lo general se manifiestan en la práctica de acuerdo con el contexto social actual; y su aplicación es compleja, sobre todo porque su aplicación depende de cómo se ejerce el poder político.

Finnemore observa cómo las organizaciones de la sociedad civil han presionado mucho para lograr un 'asiento en la mesa' de las instituciones multilaterales centradas en el Estado sobre numerosas cuestiones; y cómo las Naciones Unidas han adelantado amplios 'acuerdos de consulta' con organismos de la sociedad civil sobre ciertos temas.[25] En 2004, el Presidente del Panel de Eminentes sobre las Relaciones de las Naciones Unidas y Sociedades Civiles dedicado a estudiar la relación de las ONG con el sistema de la ONU, caracterizó el papel cada vez más importante de la sociedad civil como uno de 'los acontecimientos históricos de nuestro tiempo'.[26] Organizaciones de la sociedad civil ahora se involucran directamente en una amplia gama de temas de gobernanza y seguridad internacional, ya sea a través de la participación directa con la ONU o en relación con el áreas específica, como la OMC, órganos de tratados ambientales, minas terrestres, municiones de racimo y actividad del espacio exterior.[27] Por otra parte, este compromiso ha ayudado a producir resultados positivos, en el que se benefician enormemente el derecho internacional humanitario e internacional, en particular, de la contribución de las organizaciones de la sociedad civil. Estos últimos han ayudado a construir confianza

[23] https://www.armscontrol.org/act/2013_09/The-UN-Takes-a-Big-Step-Forward-on-Cybersecurity

[24] Informe de Gobernabilidad y Desarrollo Humano Sostenible del PNUD 1997 establece una serie de principios que con ligeras variantes, aparece en gran parte de la literatura.

[25] Finnemore, M. (2014), "New Faces, New Forms for 21st Century Multilateralism." Un documento de sesión preparado para el Simposio del Instituto Nobel en "Does the rise and fall of great powers lead to conflict and war?" Oslo, Noruega, Junio 18-22, 2014.

[26] El ex presidente de Brasil Fernando Henrique Cardoso, 'Carta de Transmisión de la Presidencia' en Nosotros los pueblos: la sociedad civil, las Naciones Unidas y gobernanza global. Informe del Grupo de Personas Eminentes sobre las Relaciones de la Sociedad Civil y las Naciones Unidas, documento de la ONU A/58/817 (11 de Junio de 2004). https://www.globalpolicy.org/empire/32340-panel-of-eminent-persons-on-united-nations-civil-society-relations-cardoso-panel. html

[27] Comunicación por correo electrónico con Duncan Hollis, agosto 15 de 2014.

entre los Estados y dentro de estos (a menudo a través de la organización y participación en procesos de medidas de construcción de confianza de track 1.5 y track 2 y fomentando el diálogo entre las partes)[28], así como 'el fomento de los tratados, la promoción de la creación de nuevas organizaciones internacionales, y el cabildeo en las capitales nacionales para obtener el consentimiento de reglas y normas internacionales más fuertes'.[29] Por otra parte, como señaló Finnemore, una mayor participación de actores adicionales en procesos multilaterales puede aumentar 'la dimensión "cualitativa" que legitima y apuntala el multilateralismo como una forma de acción política".[30] A veces, este compromiso es bien recibido por los estados; a menudo no lo es. Y en los casos en que los estados y los gobiernos nacionales no han cumplido o no han logrado un consenso sobre ciertos asuntos globales, por ejemplo, el cambio climático, las oportunidades para los actores de la sociedad civil para sugerir alternativas han aumentado.[31]

En el campo de la seguridad cibernética, acuerdos consultivos y participativos todavía son un tanto limitados. De hecho, hasta la fecha, la participación (directa o indirecta) de la sociedad civil en la elaboración de estrategias de seguridad cibernética nacional o en las normas regionales e internacionales y los procesos de medidas de construcción de confianza ha sido mínima, a pesar del hecho de que las organizaciones de la sociedad civil representan, junto con el sector privado, la academia y grupos de reflexión de política, enlaces principales en la cadena de valor de las TIC y tienen 'preocupaciones normativas' con respecto a cómo se resuelven los problemas de seguridad internacional y regional debido a las TIC.[32] De hecho, la experiencia, el conocimiento y alcance de estos grupos es fundamental para resolver o responder a muchos de los problemas técnicos básicos inherentes al entorno de las TIC, y muchas de las inseguridades y desconfianza que han surgido entre y dentro de los estados con respecto a los usos de las TIC.

Sin lugar a dudas, hay lecciones que extraer de cómo las organizaciones de la sociedad civil han apoyado los esfuerzos del gobierno para aprovechar las TIC en la respuesta a los conflictos intra-estatales y catástrofes humanitarias. Este compromiso surgió de la Declaración de Principios de la Cumbre Mundial sobre la

[28] Organizaciones como el Centro HD, CMI y similares tienen una larga trayectoria en este área al igual que muchos grupos de reflexión europeos y en Estados Unidos.

[29] Charnovitz, S. (2006). "Nongovernmental organisations and International Law.' *American Journal of International Law*, 100 (2), 348-372 (p. 348). Obtenido de http://www.jstor.org/stable/3651151. Véase también: K Raustiala, "NGOs in International Treaty-Making' in D Hollis (ed), *The Oxford Guide to Treaties* (OUP, 2012).

[30] Finnemore, M. (2014). Véase también Vedder, A. (ed) *NGO Involvement in International Governance and Policy: Sources of Legitimacy*.

[31] Ibíd. Finnemore analiza dos ejemplos básicos: El Fondo Mundial de Lucha contra el Sida, la Malaria y Tuberculosis, que es una asociación público-privada que utiliza el dinero de fundaciones filantrópicas privadas para el financiamiento de la ejecución llevada a cabo por entidades tanto gubernamentales como organizaciones no gubernamentales; y el C40 Cities Climate Leadership Group, una red de las megalópolis más grandes del mundo se centró en responder a los desafíos que plantea el cambio climático.

[32] Ibíd. Como señaló Finnemore, "ampliar la participación con nuevos tipos de actores hoy está impulsada no solo por la necesidad de eficacia (es decir, quién debe participar para construir una solución al problema), sino también por necesidades normativas (es decir, quién se ve afectado por el problema, y tiene una participación en la forma en que se resuelve).

Sociedad de la Información (CMSI) y el Plan de Acción de acompañamiento de Ginebra que incluyó un énfasis en la 'creación de confianza y seguridad en la utilización de las TIC'.[33] En 2005, bajo el Compromiso de Túnez de la CMSI, los gobiernos también se comprometieron a utilizar las TIC para promover la paz y la prevención de conflictos. El párrafo 36 del Compromiso de Túnez que lo acompaña hizo especial hincapié en el papel que las TIC pueden desempeñar en la 'identificación de situaciones de conflicto mediante sistemas de alerta temprana, prevención de conflictos, la promoción de su resolución pacífica, apoyo a la acción humanitaria, incluida la protección de civiles en los conflictos armados, facilitación de las misiones de mantenimiento de la paz, y la ayuda a la construcción de la paz y la reconstrucción post-conflicto' entre los pueblos, las comunidades y los interesados en la gestión de crisis, la ayuda humanitaria y la consolidación de la paz.[34]

A pesar de los peligros que implica, las organizaciones de la sociedad civil, en particular las que trabajan sobre el terreno, siguen desempeñando un papel fundamental llevando esos compromisos a la realidad, a través de los esfuerzos apoyados por las TIC para difundir información sobre conflictos cinéticos y apoyar la recuperación, ya sean solos, con empresas privadas de tecnología, o en conjunto con el gobierno o seguridad internacional y organizaciones humanitarias.[35] La Secretaría de la ONU también prevé la participación de entidades no gubernamentales en la ejecución de su estrategia de tecnología de comunicaciones de la información 2008 a nivel mundial.[36] Como se evidencia en el informe 'Tecnologías de la Información y la Comunicación para la Paz: El papel de las TIC en la prevención, respuesta y recuperación del conflicto', las organizaciones de la sociedad civil han desempeñado un papel activo en este sentido, sobre todo en el ámbito de la gestión de crisis.[37]

Por el contrario, las normas relacionadas con las TIC y los procesos de medidas de

[33] Véase 'Building the Information Society: A Global Challenge in the New Millennium'. Específicamente párr. Building Confidence and Security in the Use of ICTs, párrafos 35-37 específicamente en relación con la construcción de un marco de confianza; la prevención del uso de las TIC con fines incompatibles con los objetivos de mantener la estabilidad y la seguridad internacionales; y tratar con el spam en los niveles nacionales e internacionales apropiados. http://www.itu.int/wsis/docs/geneva/official/dop.html

[34] Para. 36, Compromiso de Túnez: 'We value the potential of ICTs to promote peace and to prevent conflict which, *inter alia,* negatively affects achieving development goals. ICTs can be used for identifying conflict situations through early-warning systems preventing conflicts, promoting their peaceful resolution, supporting humanitarian action, including protection of civilians in armed conflicts, facilitating peacekeeping missions, and assisting post conflict peace-building and reconstruction'. http://www. itu.int/wsis/docs2/tunis/off/7.html Para. 36 los gobiernos de Suiza y Túnez lo introdujeron en las negociaciones diplomáticas en 2004 para su aprobación como parte del compromiso de la CMSI en Túnez en 2005. La Fundación ICT4Peace (www.ict4peace.org) se estableció posteriormente en la primavera de 2006 para crear conciencia sobre el Compromiso de Túnez y promover su realización práctica en todas las etapas de la gestión de crisis.

[35] Para escuchar cómo están siendo aprovechadas las TIC para la prevención de conflictos y construcción de la paz, véase: http://www.unicef.org/education/bege_73728.html

[36] Véase la Estrategia de la Tecnología de Información y Comunicaciones de 2008 de la Secretaría de las Naciones Unidas (A/62/793 y Corr.1 y A/62/793/Add.1) y el informe de 2010 de actualización (A/65/491) disponible en: http:// daccess-ods.un.org/TMP/5780049.56245422.html y http://daccess-dds-ny.un.org/doc/UNDOC/GEN/ N10/567/93/PDF/N1056793.pdf?OpenElement respectivamente.

[37] ICT4Peace/Grupo de Tarea TICde las Naciones Unidas. Disponible en: http://bit.ly/1bR0yPI

construcción de confianza en el contexto de la seguridad internacional y regional no se han beneficiado totalmente de la participación de la sociedad civil y otros actores no gubernamentales. En 2011 ICT4Peace hizo un llamado a la participación ampliada y la puesta en común de los recursos de los diferentes interesados.[38] Sin embargo, incluso las conferencias internacionales, como la serie iniciada en Londres en 2011[39], específicamente dirigido a ampliar el diálogo de la seguridad cibernética más allá de los participantes gubernamentales, se han estancado, dejando a muchas organizaciones de la sociedad civil sin piso. De hecho, la Conferencia de Seúl sobre el ciberespacio trató de responder a la percepción de un exceso de participación en años anteriores poniéndole un tope a la cantidad de grupos no gubernamentales que podían asistir. Sin embargo, sí invitó a grupos no gubernamentales como ICT4Peace y el Consejo del Atlántico para organizar reuniones paralelas y presentar sus declaraciones en sesión plenaria.[40] Aún no está claro cómo el gobierno de los Países Bajos involucrará a la sociedad civil y otros actores no gubernamentales cuando sean los anfitriones en la próxima conferencia internacional sobre el ciberespacio en 2015.

Al mismo tiempo, es importante reconocer que las organizaciones no gubernamentales llagaron a la discusión más bien tarde. Solo recientemente vieron los vínculos que existen entre las dimensiones internacionales de seguridad de las TIC, por un lado, y los asuntos técnicos, de derechos humanos, de desarrollo y gobernanza por el otro.[41] Las organizaciones de la sociedad civil, incluidas las que trabajan en temas técnicos relacionados con Internet y también aquellas con experiencia en formulación de ley o desarrollo internacional y política comercial, pueden reunirse para ayudar a derribar las barreras a la participación y garantizar procesos multilaterales más cualitativos e incluyentes.

En 2013, se abrieron una ventanas de oportunidad en este sentido. De hecho, el Informe del Grupo de Expertos Gubernamentales de la ONU de 2013[42] reconoció el papel de la sociedad civil y del sector privado en la implementación de las normas,

[38] ICT4Peace (2011), Getting Down to Business: Realistic Goals for the Promotion of Peace in Cyberspace. Disponible en: http://ict4peace.org/%EF%BF%BCgetting-down-to-business-realistic-goals-for-the-promotion-of-peace-in-cyber-space/

[39] https://www.gov.uk/government/news/london-conference-on-cyberspace-chairs-statement

[40] Véase, por ejemplo: http://ict4peace.org/wp-content/uploads/2013/10/ICT4Peace-Statement-Seoul- Conference-on-Cyberspace-2013-1.pdf

[41] En el plano interno, los vínculos han sido mayores, como se evidencia en los informes del Relator Especial de la ONU sobre la promoción y protección del derecho a la libertad de opinión y expresión y la manera en que las organizaciones de derechos humanos y defensores de la privacidad se han involucrado con las ramas ejecutivas y legislativas sobre diferentes aspectos de la política nacional de seguridad cibernética.

[42] Para información sobre el Grupo de Expertos Gubernamentales (GGE) en materia de TIC ver Kavanagh *et al*, Baseline Review of ICT-Related Processes and Events: Implications for International and Regional Security. ICT4Peace (2014). Disponible en: http://ict4peace.org/baseline-review-of-ict-related-processes-and- events-implications-for-international-and-regional-security/; Maurer, T. (2012), Cyber Norm Emergence at the UN: An Analysis of the Activities at the UN Regarding Cyber Security. Belfer Centre for Science and International Affairs. Disponible en: http://belfercenter.ksg.harvard.edu/publication/21445/cyber_norm_emergence_at_the_united_nationsan_analysis_of_the_uns_activities_regarding_cybersecurity.html; y Tikk-Ringas, E. (2012), Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012. ICT4Peace. Disponible en: http://www.ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf

las medidas de construcción de confianza y medidas de fomento de la capacidad.[43] Más concretamente, el párrafo 12 del informe reconoce que 'aunque los Estados deben liderar al abordar estos retos, sería beneficiosa la cooperación efectiva de una participación adecuada por parte del sector privado y la sociedad civil'.[44] (Si bien podemos tener diversas interpretaciones sobre el significado del término "adecuado" y a quién le correspondería decidir qué es adecuado en este contexto, la sociedad civil y el sector privado deberían interpretarlo como una importante oportunidad para participar).

La sección detallada del informe sobre las normas, reglas y principios de comportamiento responsable por parte de los Estados[45] va un paso más allá señalando específicamente que:

> Los Estados deben alentar al sector privado y la sociedad civil para que desempeñen un papel adecuado en la mejora de la seguridad y en el uso de las TIC, incluida la seguridad de la cadena de suministro de productos y servicios TIC. (Párrafo 24)

y que

> Los Estados miembros deben estudiar la mejor manera de cooperar en la aplicación de las normas anteriores y los principios de comportamiento responsable, incluyendo el papel que pueden desempeñar el sector privado y las organizaciones de la sociedad civil. Estas normas y principios complementan la labor de las Naciones Unidas y grupos regionales y son la base para el trabajo de construir confianza. (Párrafo 25)

En referencia a las medidas de construcción de confianza e Intercambio de Información,[46] el informe señala específicamente en el párrafo 28 que 'aunque los Estados deben liderar el desarrollo de medidas de construcción de confianza, su trabajo se beneficiaría de la participación adecuada del sector privado y la sociedad civil'.[47] Combinadas, estas recomendaciones son de importancia para una mayor participación directa e indirecta.

En comparación con el informe de Grupo de Expertos Gubernamentales, la Decisión 1106 del Consejo Permanente de la OSCE (PC) sobre un "conjunto inicial de medidas de construcción de confianza para reducir los riesgos de conflicto originado por el uso de las TIC' adoptada por el Consejo Permanente del organismo regional en diciembre 2013 no menciona a la sociedad civil.[48] Sin embargo, esto no significa

[43] Véase el informe del Secretario General de la ONU 'Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security' (A/68/98*) del mes de junio de 2013 (pp.7-9)
[44] Ibíd. (p.7)
[45] Ibíd. (p.4)
[46] Ibíd. Sección IV (p.9)
[47] Ibíd. Sección IV, párr. 27 (p.9)
[48] Para una visión general de la Decisión 1106 de OSCE PC véase: Kavanagh *et al*, Baseline Review of ICT-Related Processes and Events: Implications for International and Regional Security. ICT4Peace 2014. Disponible en: http://ict4peace.org/baseline-review-of-ict-related-processes-and-events-implications-

necesariamente que la sociedad civil y otros actores fundamentales no deban representar un papel en la aplicación del conjunto inicial de medidas de construcción de confianza. En primer lugar, la Guía de la OSCE sobre medidas de construcción de confianza no militares preparada por la Secretaría de la OSCE subraya cómo las medidas de construcción de confianza idealmente deben incluir tanto las estructuras de gobierno como la sociedad civil, y esta última también tiene un papel en llegar a la sociedad más amplia en la fase de ejecución de las medidas de construcción de confianza.[49] La Guía hace hincapié en que medidas de construcción de confianza requieren 'convencimiento' por parte de la sociedad en general (es decir, el aspecto legitimante, cualitativo del proceso multilateral) si se quiere tener éxito. Mientras se mantiene realista sobre las limitaciones de la sociedad civil, la Guía destaca el importante papel de la sociedad civil en lograr ese convencimiento. En segundo lugar, la OSCE sostiene que se pueden establecer plataformas para garantizar la consulta con la sociedad civil sobre una serie de cuestiones, entre ellas las medidas de construcción de confianza. En este orden de ideas, la OSCE pretende organizar una reunión con las partes interesadas no gubernamentales para discutir sus necesidades y expectativas en relación con el proceso de medidas de construcción de confianza de la OSCE. La reunión se estableció que tendrá lugar en noviembre de 2014.[50]

En cuanto a los procesos específicos de Internet, en abril de este año, el gobierno de Brasil organizó una conferencia de múltiples partes interesadas sobre el futuro de la gobernanza de Internet en la que la sociedad civil tuvo un papel significativo (en todas las etapas de la reunión). Por otra parte, la declaración de cierre de la Conferencia presentó un conjunto de principios básicos del proceso de gobernanza de Internet enfatizando la importancia del enfoque de múltiples partes interesadas en contribuir a un marco de gobernanza de Internet incluyente, eficaz, legítimo y en evolución. Por otra parte, señaló que 'la eficacia en el tratamiento de los riesgos y amenazas a la seguridad y estabilidad de Internet depende de una estrecha cooperación entre diferentes grupos de interés'. La declaración también hizo hincapié en los principios de gobernanza abierta, participativa y basada en el consenso; la transparencia; rendición de cuentas; la inclusión y la equidad; el carácter distribuido y de colaboración de la Internet; y la participación.[51] Sin lugar a dudas estos principios son igualmente aplicables a los procesos relacionados con las TIC en el contexto de la seguridad internacional y regional.

En resumen, hay muchos precedentes en las Naciones Unidas, organizaciones regionales y otros foros internacionales para lograr un enfoque más acogedor, equitativo y eficaz para vincular a actores más allá del gobierno, es decir, la sociedad civil, así como la academia y el sector privado, en una gama de normas y procesos de medidas de construcción de confianza. Como viene siendo cada vez más

for-international-and-regional-security/

[49] Guía de la OSCE sobre Medidas de creación de confianza no militares (2013). Disponible en: http://www.osce.org/cpc/91082

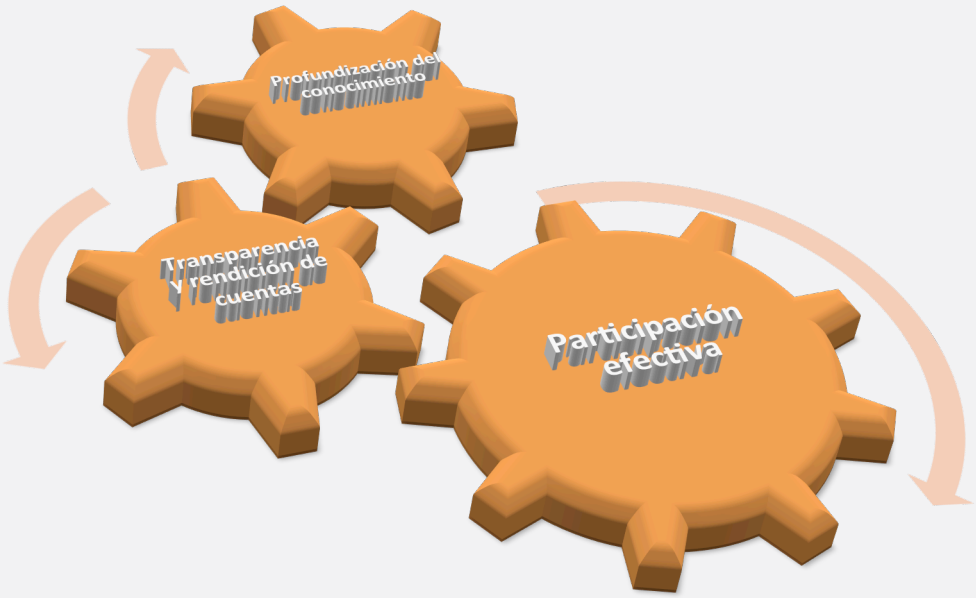
[50] Comunicación con la OSCE, 11 de agosto 2014.

[51] NETmundial Declaración de las múltiples partes interesadas, 24 de abril 2014. http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf

evidente, la seguridad cibernética sin duda no deberá ser la excepción.

3. CUÁL ES EL PAPEL, POR LO TANTO, PARA LA SOCIEDAD CIVIL EN LA PROMOCIÓN DE NORMAS Y CBM EN ESTE CAMPO

La sociedad civil puede ayudar a profundizar el cambio en: normas y medidas de construcción de confianza relacionadas con las TIC en tres áreas separadas, pero superpuestas: i) la participación efectiva; ii) Fomento de la Transparencia y Rendición de Cuentas; y iii) Profundización del Conocimiento. Combinadas, estas medidas pueden fortalecer la legitimidad y la sostenibilidad de los procesos en curso; garantizar que asuntos normativos más amplios son atendidos, y que la experiencia técnica adecuada está utilizada cuando se están buscando soluciones; y en última instancia, ayudar a construir confianza entre los Estados y entre el Estado y la sociedad.



PARTICIPACIÓN EFECTIVA

Como se señaló anteriormente, hay muchos precedentes en la ONU y las organizaciones regionales para lograr un enfoque más acogedor, equitativo y eficaz para involucrar a la sociedad civil en cuestiones relativas a la gobernanza mundial y seguridad internacional. Dada la naturaleza del ecosistema, la seguridad cibernética no debe ser una excepción. Ciertamente, la gama de asuntos de legitimidad y normativos, así como los aspectos técnicos involucrados requieren de un compromiso mucho más profundo de la sociedad civil que otras áreas. Uno de los principales objetivos de la sociedad civil debe ser, por tanto, presionar por el derecho de influir directa o indirectamente en las discusiones multilaterales que pretenden llegar a un acuerdo sobre las normas y las medidas de construcción de confianza en este área. Mientras que se han planteado preocupaciones legítimas de seguridad nacional en relación con algunos de los aspectos no públicos de los procesos en el campo de la seguridad cibernética (especialmente ejercicios de creación de confianza entre los militares), hay suficientes ejemplos de cómo la sociedad civil puede participar. Por ejemplo:

- Las organizaciones de la sociedad civil pueden solicitar u organizar audiencias antes y después de la participación del gobierno en las medidas de construcción de confianza, normas y otros procesos relacionados con la seguridad cibernética, con el gobierno y el parlamento. Esto se hace en otros ámbitos relacionados con la paz y la seguridad internacionales, y no hay razón para que no se pueda hacer con respecto a la seguridad cibernética.

- También pueden cabildear por su participación directa o indirecta en los procesos de medidas de construcción de confianza y normas de acuerdo con el resultado del informe 2013 GGE. Por ejemplo, se puede incluir la representación de la sociedad civil en las delegaciones gubernamentales a las discusiones sobre medidas de construcción de confianza y normativa. Estados Unidos incluyó una fuerte representación de la sociedad civil en su delegación a la reunión CMTI en Dubai 2012; el gobierno de Estonia ha incluido un representante de un grupo de expertos internacionales en su delegación a la última GGE y hará lo mismo en el actual (aunque el representante académico que había participado en los dos últimos GEI ha sido reemplazado por un abogado del gobierno); el gobierno de la República de Corea incluyó un miembro de uno de los principales grupos de reflexión del país, ETRI y un profesor de derecho en el Centro de Ley Cibernética de la Universidad de Corea en calidad de asesores en su Delegación en el GGE 2014; ICT4Peace apoyó al gobierno de Suiza en las discusiones de la OSCE sobre las medidas de construcción de confianza; y la sociedad civil y la academia han formado parte de las discusiones en curso de UE-China sobre medidas de construcción de confianza.

- La sociedad civil puede solicitar el establecimiento de estructuras como una junta o panel de asesoría para acompañar el trabajo del nuevo Grupo de Expertos Gubernamentales que comenzó a trabajar en junio de 2014. Este consejo asesor puede estar integrado por personas representativas de la sociedad civil, la industria y la academia, invitado por el Secretario General de la ONU para aportar asesoramiento especializado al Grupo de Expertos Gubernamentales y gobiernos nacionales cuando se requiera (por ejemplo, en relación con los párrafos 24 y 25, del apartado sobre normas, reglas y principios de comportamiento responsable por los Estados) del informe del Grupo de Expertos Gubernamentales de la ONU de 2013, que hace referencia específicamente a un papel de la sociedad civil y el sector privado en el apoyo a la aplicación del paquete de normas y principios que se recomienda en el informe).

- La sección de Medidas de construcción de confianza y el intercambio de información en el informe de 2013 GGE pide 'Intercambios de información y comunicación entre los equipos de respuesta de emergencia informática nacional (CERT) de forma bilateral, al interior de las comunidades del CERT, y en otros foros, para apoyar el diálogo a nivel político y de políticas'. También sugiere una 'mayor cooperación para abordar los incidentes que pudieran afectar a las TIC o las infraestructuras críticas que se basan en sistemas de control industrial basados en las TIC', señalando que 'esto podría incluir directrices y mejores prácticas entre los Estados contra las interrupciones perpetradas por actores no estatales'.[52] Ciertamente CERT no gubernamentales son quizás un ejemplo de una de las formas más directas de participación de la sociedad civil en la respuesta a las amenazas y vulnerabilidades en los sistemas en red. Tienen un profundo conocimiento de las cuestiones técnicas a la mano, están bien posicionados para desarrollar directrices y registrar las buenas prácticas, y tienen una amplia experiencia en la construcción de confianza entre las comunidades. Vale decir que las normas y procesos de medidas de construcción de confianza en curso se beneficiarían significativamente de una participación más profunda con estos CERT.

- Las organizaciones de la sociedad civil pueden participar en/apoyar los esfuerzos de creación de capacidad o incluso organizar eventos en conjunto con las autoridades nacionales que están diseñadas para implementar medidas de construcción de confianza existentes. Por ejemplo, el conjunto inicial de las medidas de construcción de confianza de la OSCE alienta a los Estados, entre otras cosas, a 'compartir información sobre las medidas que se han adoptado para garantizar un Internet abierto, interoperable, seguro y confiable'.[53] Esta medida, en particular, podrían beneficiarse significativamente de una participación fuerte de la sociedad civil y del sector privado.

[52] 2013 GGE Report, para. 27(iv) and v)

[53] OSCE 'Initial Set of OSCE Confidence Building Measures to Reduce the Risk of Conflicts Stemming from the Use of Information Communications Technologies.' PC.DEC/1106 of 3 December 2013 (para.4) Disponible en: http://www.osce.org/pc/109168?download=true

- El informe 2013 GGE también incluye una sección sobre creación de capacidad, destacando la importancia de involucrar a otras partes interesadas en los esfuerzos de creación de capacidad. Ya grupos de la sociedad civil y la academia están trabajando con los gobiernos y las organizaciones internacionales para volver realidad estos compromisos y recomendaciones. Por ejemplo, ICT4Peace está comenzando un nuevo proyecto de creación de capacidad con diferentes organizaciones regionales destinados a nivelar el campo de juego, asegurando que todas las regiones están sustancialmente y técnicamente equipados para participar en procesos de medidas de construcción de confianza y normas internacionales y regionales relacionadas con las TIC. Otros grupos no gubernamentales que participan en los esfuerzos de desarrollo de capacidades incluyen el Centro de Capacidad de Seguridad Cibernética de la Universidad de Oxford.[54] Algunos grupos de la sociedad civil podrían tomar otro rumbo, por ejemplo, el seguimiento de la eficacia real de los esfuerzos de creación de capacidad en este área en la contribución a la seguridad internacional y regional, así como el desarrollo a largo plazo.
- Por último, no todos compromiso de la sociedad civil es eficaz, ni es siempre productivo. Si la sociedad civil ha de participar en este área, también deberá desarrollar mecanismos con otras partes interesadas para supervisar y evaluar sus propias contribuciones.

FOMENTO DE LA TRANSPARENCIA Y RENDICIÓN DE CUENTAS

Monitoreo de la política y la acción del gobierno y la promoción de las normas nacionales e internacionales

Abundan los ejemplos de cómo las organizaciones de la sociedad civil pueden supervisar las acciones del gobierno y el uso de los datos que recoge para influir en un cambio de política, establecer normas y estándares, etc. Por ejemplo, la participación de la sociedad civil en la elaboración de normas que rigen las transferencias de armas[55] o el uso de armas específicas ha sido bastante efectiva, a pesar de las dificultades inherentes al trabajo en este área. El proceso que condujo al Tratado de Minas de Ottawa (Convención sobre la prohibición de minas antipersonales) también surgió de una fuerte participación de la sociedad civil,[56] al

[54] Véase: http://www.oxfordmartin.ox.ac.uk/institutes/cybersecurity

[55] Por ejemplo, la ONG Saferworld con sede en Reino Unido ha desempeñado un papel activo en informar a los Parlamentos de la UE sobre la cuestión de las transferencias de armas tradicionales y para influir en las decisiones de política pertinentes. Esto se hizo a través del desarrollo de dos Blackbooks sobre las transferencias de armas a países europeos destinados a contribuir a la revisión de la Posición común de la UE sobre exportaciones de armas. Los dos Blackbooks son: '*Rhetoric or Restraint?' Trade in military equipment under the EU transfer control system'* publicado en 2010 y '*Lessons from MENA: Appraising EU transfer of military and security equipment to the Middle East and North Africa'* publicado en noviembre de 2011. Este último cubría la construcción de vehículos blindados en Sudán bajo la producción bajo licencia con empresas alemanas y francesas y fue respondido con bastante rapidez con el cierre de esa instalación de construcción. Comunicación con Saferworld, diciembre de 2012 y julio 2014.

[56] Tanto el papel de la sociedad civil y algunos de los desafíos en relación con su participación en este

igual que el proceso de elaboración del tratado de prohibición de las bombas de racimo.[57] En el campo de las TIC y la seguridad internacional, la participación de la sociedad civil limitada es todavía, aunque creciente. Por ejemplo:

- Grupos de la sociedad civil han hecho reiterados llamamientos a los gobiernos para regular la exportación de tecnología de vigilancia a los usuarios finales con registros cuestionables de derechos humanos.[58] Su justificación es que los controles eficaces de exportación de este tipo de tecnologías de doble uso asegurará que podrían ser utilizados para facilitar violaciones de los derechos humanos. Algunos argumentan que la reglamentación en esta materia no tiene sentido.[59] Al mismo tiempo, hay todavía insuficiente análisis de la dimensión política de este problema y el grado en que los reglamentos de control de exportaciones existentes cubren esta tecnología. Organizaciones de la sociedad civil pueden desempeñar un papel importante al continuar monitorear y documentar las prácticas gubernamentales y de la industria, identificando nuevas brechas y proporcionando análisis más profundo de políticas y tecnológico para la elaboración de políticas.

- En cuanto a cuestiones más amplias relacionadas con los usos militares de las TIC (o guerra cibernética), pasos hacia el establecimiento de normas pueden incluir trabajar con los gobiernos y otros actores en el marco, la redefinición y la comunicación de las preocupaciones y asuntos normativos asociados.[60] (Ver ejemplos de DIH en la siguiente sección en la profundización del conocimiento)

- La acción de la sociedad civil también puede implicar hacer campaña *en contra de* las políticas y acciones gubernamentales que considera que son de preocupación normativa para grupos específicos o la sociedad en general. Por ejemplo, muchas organizaciones de la sociedad civil han desempeñado un papel importante en la respuesta a las preocupaciones de derechos de datos a nivel nacional y la conformación del comportamiento del Estado en este tema.[61] Del mismo modo, los grupos de la sociedad civil y otros actores no estatales como la academia y centros de investigación que se ocupan de

proceso se analizan en: Short, N. (2009). The Role of NGOs in the Ottawa Process to Ban Landmines. *International Negotiation* 4: 481-500, 1999. http://faculty.maxwell.syr.edu/rdenever/IntlSecurity2008_docs/Short_ NGOsOttawa.pdf

[57] Para ver un debate sobre el papel de la sociedad civil en este proceso, consulte Bolton, M. y Nash, T. (2010), The Role of Middle Power-NGO Coalitions in Global Policy: The Case of the Cluster Munitions Ban.' *Global Policy*, Vol. 1, número 2, mayo de 2010.

[58] Maurer *et al* (2014).

[59] Véase, por ejemplo, Lewis, J.A. (2010), "'Multilateral Agreements to Constrain Cyberconflict,' Arms Control Association. https://www.armscontrol.org/print/4261

[60] Para ejemplos de participación de la sociedad civil en algunos de esos lugares véase Rappert *et al* (2012), 'The roles of civil society in the development of standards around new weapons and other technologies of warfare.' *International Review of the Red Cross.* http://www.icrc.org/eng/assets/files/review/2012/irrc-886- rappert-moyes-crowe-nash.pdf

[61] Por ejemplo, la campaña de la sociedad civil para rechazar las propuestas estadounidenses para regular la infracción de derechos de autor/la piratería en línea a través de la Stop Online Piracy Act (SOPA) y la Ley de Protección de IP (PIPA), llevó a una amplia gama de protestas impulsadas por compañías y organizadas por la sociedad civil, incluyendo el oscurecimiento de Wikipedia por un día.

cuestiones de privacidad pueden trabajar juntos para cabildear y supervisar la aplicación de las recomendaciones presentadas en el reciente informe de la Oficina del Alto Comisionado para los Derechos Humanos sobre el derecho a la privacidad en la era digital.[62] [63]

Hasta hace muy poco, muy poca información sobre los procesos internacionales, regionales y bilaterales en materia de seguridad cibernética era de dominio público. En gran medida, muchas de estas discusiones han recibido un escrutinio limitado de fuentes tradicionales de peso y contrapeso, incluida la sociedad civil. Como medio para superar este desafío, los grupos de la sociedad civil pueden:

- Desarrollar herramientas para supervisar el papel de su propio gobierno en las discusiones sobre medidas de construcción de confianza y normas internacionales, regionales y bilaterales y hacer que el conocimiento sobre los avances o retrocesos en las normas internacionales y regionales y los procesos de medidas de construcción de confianza estén fácilmente disponibles para el público, trabajando con los medios de comunicación y otros grupos para organizar discusiones públicas en torno a ellos. Por ejemplo, en mayo de este año, ICT4Peace publicó su primer examen anual de los acontecimientos y procesos relacionados con las TIC que tienen implicaciones para la seguridad internacional y regional.[64] Otras organizaciones de la sociedad civil han emprendido esfuerzos similares relacionadas con las TIC. Por ejemplo, Global Partners Digital publicó recientemente un extenso informe sobre los procesos relacionados con la gobernanza de Internet destacando algunas de las principales áreas de tensión y discordia en este área.[65]

- En otro nivel, organizaciones de la sociedad civil pueden ayudar a desarrollar y promover estándares comunes, idealmente reconocidos internacionalmente para la transparencia informativa en materia de seguridad cibernética nacional e internacional. El principal reto es determinar en qué tipo de informes de transparencia deben centrarse: Por ejemplo, si la atención se centra en la promoción de una mayor transparencia en las prácticas de supervisión y vigilancia del gobierno, debería la información centrarse en los aspectos más específicos del acceso SIGINT a datos o en cuestiones más extensas como períodos de retención de datos, retiradas, etc.? En cualquier caso, las organizaciones de la sociedad civil que trabajan con las instituciones gubernamentales relevantes y/o la empresa privada y la academia están bien posicionadas para adelantar tanto las formas específicas como extensas de la

[62] Meyer, P. "Surveillance: A Potential 'Chilling Effect' on Human Rights? Report on 'Right to privacy' calls for independent civilian oversight agency". Consejo Internacional de Canadá, 15 de agosto de 2014. Disponible aquí: http://opencanada.org/features/the-think-tank/comments/surveillance-a-potential-chilling- effect-on-human-rights/

[63] Derecho a la privacidad en la era digital, Informe de la Oficina del Alto Comisionado para los Derechos Humanos (A/HRC/27/37) de 30 de junio de 2014.

[64] Cf. la nota 42 supra.

[65] Internet Governance: Mapping the Battleground, Global Partners & Associates (2013). http://www.gp-digital.org/wp-content/uploads/pubs/Internet-Governance-Mapping-the-Battleground.final_1.pdf

transparencia informativa.[66]

Monitoreo de los gastos del gobierno

De hecho, la mayoría de los fondos públicos canalizados a responder a los riesgos y las vulnerabilidades relacionadas con la cibernética que representan una amenaza a la seguridad internacional se están invirtiendo en las áreas militares de defensa y ofensa, o en el campo de la inteligencia, a menudo sin suficiente justificación. Mientras que la presentación de información sobre el gasto en este área pública podría ser difícil en virtud de i) las dificultades en el desglose del gasto en este campo, en rubros presupuestales específicos y coherentes; y ii) el hecho de que gran parte de la información relevante está clasificada para fines de seguridad nacional, es necesario que haya algún tipo de transparencia y rendición de cuentas para tranquilizar a los grupos nacionales (de cara a las libertades civiles, así como las preocupaciones de eficacia institucional), por un lado, y fomentar la confianza entre los Estados, por otra.

- En primer lugar, a pesar de la naturaleza confidencial de los gastos militares en este área, la sociedad civil puede aún desempeñar un papel importante de defensa, incluso con comisiones parlamentarias especializadas, para asegurar una mínima transparencia y rendición de cuentas del gasto público. En este sentido, las organizaciones de la sociedad civil pueden presionar para que se publiquen los detalles presupuestales de alto nivel, por ejemplo, el presupuesto asignado a las "secciones" encargadas de las operaciones defensivas (no es necesario que este nivel de detalle presupuestal sea confidencial, incluso si lo fueran otros rubros más específicos). De igual forma, organizaciones de la sociedad civil pueden impulsar o supervisar la rendición de cuentas de alto nivel. El estudio de informes como los informes del Comisionado de Interceptación de Comunicaciones del Reino Unido,[67] que indican anualmente la rendición de cuentas dentro de los organismos de inteligencia, podría ser de gran apoyo en este sentido.

- En segundo lugar, las organizaciones de la sociedad civil pueden abogar por un equilibrio adecuado de las inversiones entre los diferentes ámbitos de políticas, aunque estén superpuestas (seguridad/defensa, gobernanza, desarrollo y protección y promoción de los derechos humanos).

Cada una de estas áreas requeriría la existencia previa de un régimen de divulgación de información de trabajo (incluida la legislación de libertad de información/acceso a la información). Por lo tanto, en los países donde este último está ausente o carece de aplicación efectiva, estos esfuerzos deben estar vinculadas a la gestión de la construcción del Estado en general y/o construcción de la democracia. Tales

[66] Comunicación por correo electrónico con Chrisopher Parsons, becario de postdoctorado, Citizen Lab de la Universidad de Toronto. 13 de agosto 2014.

[67] Véase, por ejemplo: Informe Anual del Comisionado de la interceptación de las comunicaciones de 2013. http://www.iocco-uk.info/docs/2013%20Annual%20Report%20of%20the%20IOCC%20Accessible%20Version.pdf

esfuerzos de defensa deberían combinarse con estrategias dirigidas a influir en la atención del público, ejerciendo presión en vías legales alternativos, abogando por espacios de denuncia de irregularidades, etc.[68]

PROFUNDIZACIÓN DEL CONOCIMIENTO

Mejorar el conocimiento y el intercambio de información es fundamental para la construcción de un entorno TIC seguro y resistente, y para el fortalecimiento de la confianza entre los Estados. Con este fin, la sociedad civil puede:

- Trabajar más estrechamente con el sector académico y el sector privado para garantizar que la investigación basada en la evidencia se ponga a disposición de los representantes gubernamentales que participan en debates de las normas y medios de construcción de confianza, por un lado; y que estará a disposición del público en general, por otro. Ya existen ejemplos de este tipo de iniciativas:

  - En junio de 2014, expertos de los gobiernos, la sociedad civil y la industria asistieron a una reunión organizada por el Centro de Estudios Estratégicos e Internacionales (CSIS) antes de la iniciación de los trabajos del nuevo Grupo de Expertos Gubernamentales (GGE) de la ONU. El objetivo de la reunión era abordar los temas clave relacionados con seguridad [cibernética] internacional y adelantar un debate en profundidad entre expertos gubernamentales y no gubernamentales sobre estos temas como un medio para el desarrollo de un entendimiento común y tener en cuenta la gama de posibles medidas de cooperación propuesta en GGE anteriores.

  - Desde 2011, un consorcio formado por MIT, Harvard y la Citizen Lab de la Universidad de Toronto ha reunido a diferentes partes interesadas del gobierno, la academia, la sociedad civil y el sector privado para discutir normas y medios de construcción de confianza para el ciberespacio. El resultado de estas reuniones ha servido como insumo útil para las discusiones internacionales y regionales, mientras que las reuniones mismas han servido como una importante plataforma para la creación de redes y la profundización de conocimientos entre sectores y regiones sobre temas específicos relacionados con la seguridad cibernética.[69]

  - En junio de 2013, ICT4Peace organizó un taller sobre medidas de construcción de confianza y opciones para la seguridad cibernética internacional y regional. Los participantes en el taller de la sociedad civil, el gobierno, la academia y el sector privado de diferentes regiones fue

[68] Comunicación por correo electrónico con Chrisopher Parsons, 13 de agosto 2014.

[69] Véase Hurwitz, Roger (2012), An Augmented Summary of the Harvard, MIT and University of Toronto Cyber Norms Workshop. Disponible en: http://ecir.mit.edu/images/stories/augmented-summary-4%201.pdf

importante, sobre todo porque cada uno trajo perspectivas valiosas de su propia experiencia institucional al interior de sus propias realidades regionales y nacionales. Los participantes del taller elaboraron una lista exhaustiva de las medidas de construcción de confianza potenciales en áreas principales: medidas de transparencia; medidas de cooperación; mecanismos de comunicación y colaboración; medidas de contención; y medidas de cumplimiento y vigilancia para hacer frente a los desafíos relacionados con las TIC hoy. También destacaron las áreas donde ha habido progreso, cuellos de botella clave identificados (tanto políticos como técnicos) y señalaron los procesos en curso, como el UNGGE, la OSCE o el Foro Regional de la ASEAN (ARF), que ya incluyen la sociedad civil, el sector privado o la academia de una forma u otra en sus procesos relacionados con medidas de construcción de confianza.[70] El Consejo del Atlántico organizó una reunión similar sobre medidas de construcción de confianza con expertos de los países de la OTAN en 2014.

- También en 2013, un grupo de expertos en derecho internacional privado terminaron su trabajo en el Manual de Tallin sobre el Derecho Internacional aplicable a la Guerra cibernética.[71] El manual explora la aplicabilidad del derecho internacional humanitario y las doctrinas de jus ad bellum a los conflictos cibernéticos. Si bien hay argumentos jurídicos y políticos en contra de algunas de las aplicaciones del derecho internacional propuesto por el grupo, el Manual de Tallin sin embargo, ha contribuido de forma importante a la discusión de cómo podría aplicarse el derecho internacional en y para el ciberespacio. A través de su trabajo en Nuevas Tecnologías y Derecho Internacional[72] el Comité Internacional de la Cruz Roja (CICR) también está ayudando a abrir camino importante en este área.

Además, las organizaciones de la sociedad civil pueden:

- Desarrollar vínculos más fuertes con el sector privado, la academia y grupos de reflexión sobre políticas para identificar las brechas de conocimiento o profundizar la base de conocimientos en áreas específicas técnicas o de políticas, e incluir los hallazgos fundamentales en las discusiones y procesos de medidas de construcción de confianza y normas. Por ejemplo, un número de grupos de reflexión de políticas y las organizaciones de la sociedad civil están apoyando el trabajo de Track 1.5 y Track 2 en este campo. Sería útil que estas organizaciones compartan sus experiencias, como un medio para identificar con mayor eficacia las buenas prácticas y difundirlas, así como avanzar en este

[70] Véase Informe ICT4Peace: International Dialogue on Confidence Building Measures (CBMs) and International Cyber Security – ETH Zurich, 20 al 21 junio de 2013. Disponible en: http://ict4peace.org/ict4peace-global-dialogue-on-confidence-building-measures-and-international-cyber-security/

[71] El Manual ha sido elaborado por el Grupo Internacional de Expertos ante la invitación del Centro de Excelencia de Defensa Cibernética Cooperativa de la OTAN. General Schmitt, Michael M. (ed.), The Tallinn Manual on the International Law Applicable to Cyber Warfare. Disponible en: http://www.ccdcoe.org/tallinn-manual. html

[72] Véase: http://www.icrc.org/eng/war-and-law/contemporary-challenges-for-ihl/ihl-new-technologies/index.jsp

campo.

- Trabajar con el gobierno, el parlamento, la academia y la industria para asegurar las interrelaciones entre los diferentes ámbitos de políticas, a saber, la seguridad, la gobernanza, el desarrollo y los derechos humanos. Como se señaló anteriormente, la Revisión de Procesos y Eventos relacionados con las TIC del ICT4Peace avanzó de manera importante en este sentido.

- Por último, la sociedad civil puede ayudar a profundizar la comprensión de las dinámicas y diferencias culturales como un medio para generar confianza en el ciberespacio y diferentes retos de la seguridad cibernética. De hecho, aún ocurren malentendidos importantes (muchos de ellos culturales) en el área de la seguridad cibernética, que puede conducir a la intensificación de las tensiones entre Estados y entre los Estados y los ciudadanos si se deja sin resolver.

CONSIDERACIONES FINALES

La sociedad civil tiene un papel importante por desempeñar en la promoción de normas y medidas de construcción de confianza para los usos de las TIC en el contexto de la seguridad internacional y regional. Hay suficientes precedentes de la participación de la sociedad civil sobre otros asuntos de seguridad internacional y regional que justifican su participación en este área. Por otra parte, la naturaleza misma de las TIC/ecosistema del ciberespacio hace que su compromiso sea necesario (así como el de la academia y el sector privado), no solo para garantizar procesos multilaterales más cualitativos, sino también para asegurar que ciertas preocupaciones normativas son atendidas, y que se aproveche la experiencia técnica apropiada cuando se estén buscando soluciones. Combinados, estos últimos pueden ayudar a fomentar la confianza entre los Estados y entre el Estado y la sociedad. En algunos aspectos, la sociedad civil ya se está comprometiendo, pero se necesita un mayor esfuerzo por parte de los gobiernos y la sociedad civil. El Informe GGE de 2013 y la Decisión de la OSCE PC proporcionan una importante oportunidad para profundizar es ese compromiso.

LOS AUTORES

Camino Kavanagh está terminando un Ph.D. en el Departamento de Estudios de Guerra del Kings College de Londres, donde su atención se centra en tecnologías de la información y la transformación en asuntos estratégicos. Se desempeña como asesora de varias organizaciones, entre ellas la Fundación ICT4Peace y el Comité Nacional de Nueva York de Política Exterior de Estados Unidos (NCAFP) para el que ha desarrollado una serie anual de mesa redonda sobre la seguridad cibernética y la política exterior estadounidense. Su experiencia profesional incluye unos quince años trabajando en situaciones de conflicto y post-conflicto como un practicante y desde una perspectiva de políticas. Ella regularmente presta asesoría para agencias internacionales y gubernamentales, y trabaja entre Nueva York, Bamako y Londres.

Dr. Daniel Stauffacher, ex embajador de Suiza, tiene una Maestría en Asuntos Económicos Internacionales de la Universidad de Columbia, Nueva York y un doctorado en leyes de derecho de autor y la de medios de difusión de la Universidad de Zúrich. Él trabajó para la corte del distrito de Zúrich, y fue Director General de una empresa editorial antes de unirse a las Naciones Unidas en Nueva York, Laos y China (1982 - 1990) y el Gobierno de Suiza (1990-2006). Para este último era, entre otras cosas, responsable de la atención y la preparación de la Cumbre Mundial de la ONU sobre la Sociedad de la Información (CMSI), celebrada en Ginebra en 2003 y Túnez en 2005. Fue miembro de la Fuerza de Tarea de las Tecnologías de Información y Comunicaciones (TIC) del ex Secretario General de la ONU, Kofi Annan y es también el fundador y presidente de la Fundación ICT4Peace (www.ict4peace.org) y director fundador de la World Wide Web Foundation Board (www.webfoundation.org). Desde 2007 se ha desempeñado como asesor de varios gobiernos y la ONU en la mejora de los Sistemas de Gestión de Información de Crisis (CIMS) y ayudó a desarrollar la Estrategia de Gestión de Información de Crisis de las Naciones Unidas. Desde 2006, él y sus colegas en ICT4Peace han solicitado y participado en procesos internacionales y regionales para mantener un ciberespacio abierto, gratuito y seguro y han publicado una serie de publicaciones en apoyo de tales procesos (véase más adelante).

ACERCA DE LA FUNDACIÓN ICT4Peace

La Fundación ICT4Peace www.ict4peace.org se puso en marcha a raíz de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) en Ginebra en 2003 y tiene como objetivo facilitar una mejor, eficaz y sostenible comunicación entre los gobiernos, los pueblos, las comunidades y los interesados en la prevención de conflictos, la mediación y la construcción de la paz a través de una mejor comprensión y una mayor aplicación de las TIC. El Programa ICT4Peace de Derechos y seguridad en el ciberespacio se inició en 2011. ICT4Peace está interesada en seguir, apoyar y liderar los esfuerzos bilaterales y multilaterales, diplomáticos, legales y de políticas para lograr un ciberespacio seguro, próspero y abierto. Se pueden encontrar ejemplos de publicaciones de ICT4Peace en: http://ict4peace.org/?p=1076 e incluye:

- Revisión de línea de base de los Procesos y Eventos relacionados con las TIC: Implicaciones para la seguridad internacional y regional (2014)
- ¿Qué sigue? Medidas de Construcción de Confianza en el Ciberespacio (2013)
- El alcance del poder suave en respuesta a los Retos de Seguridad Cibernética Internacional (2013)
- Una visión general de procesos globales y regionales, agendas e instrumentos (2013)
- Documento de ICT4Peace sobre las consultas a Grupos de Expertos Gubernamentales (GGE) sobre seguridad cibernética en la ONU en Nueva York (2012)
- Manos a la obra: Las metas realistas para la promoción de la paz en el ciberespacio (2011)

ICT for peace FOUNDATION