LA BÚSQUEDA DE LA PAZ EN EL CIBERESPACIO

Unión Internacional de Telecomunicaciones

La búsqueda de la Paz en el Ciberespacio

Por Dr. Hamadoun I. Touré

Secretario General de la Unión Internacional de Telecomunicaciones

y el

Panel Permanente para la Supervisión de la Seguridad de la Información

Federación Mundial de Científicos

Enero de 2011

Aviso legal

Los autores mantienen los derechos de autor sobre sus obras a título individual. Cuando corresponde se citan las fuentes de terceros. La Unión Internacional de Telecomunicaciones (UIT) no se hace responsable de los contenidos procedentes de fuentes exteriores, incluidos los sitios web citados como referencia en esta publicación.

Ni la UIT ni ninguna persona que actúe en su nombre se hacen responsables de la utilización que pudiera hacerse de la información recogida en esta publicación.

Limitación de responsabilidad

Los capítulos de esta publicación representan los puntos de vista de cada autor, que no cuentan con el respaldo ni pretenden representar los puntos de vista de ninguna organización en la que estén empleados o a la que estén afiliados. La mención y las referencias relativas a países, empresas, productos, iniciativas o directivas particulares no implican en modo alguno el refrendo o la recomendación de los mismos por la UIT, los autores, o cualquier otra organización en la que los autores estén empleados o a la que estén afiliados, con preferencia sobre otros de naturaleza similar que no se mencionan.

Agradecimientos

El Secretario General de la UIT y la Federación Mundial de Científicos desean dar las gracias a Jody Westby, Henning Wegener, y a todos los autores que han hecho posible la recopilación de sus puntos de vista sobre este incipiente asunto de interés mundial. El Secretario General también expresa su agradecimiento al Profesor Antonino Zichichi, Presidente de la WFS, así como su sincera gratitud a Alexander Ntoko, Jefe de la División de Estrategia de la Unión, y muy especialmente a JeoungHee Kim, que se encargó de dirigir y coordinar esta publicación; a Rebekah Lewis, Deepti Venkateswar, Preetam Maloor, Marco Obiso y Elizabeth Aschenbrener; a Claude Briand y su equipo; y a las numerosas personas de la UIT y la WFS sin cuya contribución esta publicación no hubiera sido posible.

Si tiene algún comentario que formular, puede dirigirse a la División de Estrategia de la Unión, Unión Internacional de Telecomunicaciones, en la dirección strategy@itu.int.

ÍNDICE

Página

Abreviaturas ..... **iii**

Acerca de la Unión Internacional de Telecomunicaciones y la Agenda sobre Ciberseguridad Global ..... **v**

Acerca de la Federación Mundial de Científicos y su Panel Permanente para la Supervisión de la Seguridad de la Información ..... **vii**

Preámbulo (Por Hamadoun I. Touré, Antonino Zichichi)..... **xii**

1 Introducción (Por Jody R. Westby)..... **1**

2 El ciberespacio y la amenaza de guerra cibernética (Por Hamadoun I. Touré) **7**

3 Dependencia y confianza social (Por Jacques Bus) **15**

3.1 La dependencia de las sociedades modernas respecto de las TIC e Internet *15*

3.2 Repercusiones socioeconómicas de la ciberdelincuencia..... *28*

4 Tendencias y amenazas tecnológicas **33**

4.1 Potencial actual, tendencias y amenazas (Por Axel Lehmann, Vladimir Britkov, Jacques Bus)..... *33*

4.2 Censura de Internet por los Gobiernos: Ciberrepresión (Por Henning Wegener) *46*

5 Ciberconflicto y estabilidad geocibernética..... **57**

5.1 Ciberconflicto (Por Giancarlo A. Barletta, William A. Barletta, Vitali N. Tsygichko) *57*

5.2 Un llamamiento a la estabilidad geocibernética (Por Jody R. Westby) *73*

6 Ciberespacio (Por Henning Wegener) **86**

Un concepto de ciberespacio..... *86*

Página

7 Respuesta internacional a la ciberguerra (Por Hamadoun I.Touré) **96**

7.1 Políticas y planteamientos nacionales *96*

7.2 Respuestas internacionales recientes *102*

7.3 Necesidad de un marco internacional *107*

7.4 Propuestas de principios internacionales en el ciberespacio *111*

8 Agenda de la UIT sobre ciberseguridad global (PorHamadoun I.Touré) **116**

9 Declaración de Erice sobre Principios de Estabilidad y Paz Cibernéticas (Por Federación Mundial de Científicos) **123**

10 Conclusión (Por Jody R. Westby) **126**

Abreviaturas

SIA	Sistemas de Información Automatizados
ARPA	Advanced Research Projects Agency (Agencia de Proyectos de Investigación Avanzada) (Departamento de Defensa de los Estados Unidos)
C3	Mando, Control y Comunicaciones
CoE	Consejo de Europa
PIeL	Iniciativa de Protección de la Infancia en Línea
CRS	Congressional Research Service (Estados Unidos)
CSCW	Trabajo en grupo asistido por computador
DARPA	Defense Advanced Research Projects Agency (Departamento de Defensa de los Estados Unidos)
DNS	Sistema de nombres de dominio
ECOSOC	Consejo Económico y Social (ONU)
ESCAPE	Plataforma de Aplicación para la Colaboración Electrónica Segura entre Expertos (IMPACT)
UE	Unión Europea
FG Smart	Grupo Temático sobre las Redes Inteligentes
FTC	Federal Trade Commission (Estados Unidos)
ACG	Agenda sobre Ciberseguridad Global (UIT)
GRC	Centro de Respuesta Global (IMPACT)
CDH	Comité de Derechos Humanos (CDH)
TIC	Tecnologías de la información y la comunicación
FGI	Foro sobre el Gobierno de Internet
IMPACT	Alianza Internacional Multilateral contra las Ciberamenazas (Malasia)
IP	Protocolo Internet
ISOC	Internet Society
TI	Tecnología de la información
RTI	Reglamento de las Telecomunicaciones Internacionales (UIT)
UIT	Unión Internacional de Telecomunicaciones
UIT-T	Sector de Normalización de las Telecomunicaciones de la UIT
LOAC	Derecho de los conflictos armados
MIT	Massachusetts Institute of Technology
OTAN	Organización del Tratado del Atlántico Norte
NEWS	Sistema de alerta temprana en red (IMPACT)

TNP	Tratado sobre la no proliferación de las armas nucleares
NSF	National Science Foundation
RFID	Identificación por radiofrecuencias
PDA	Agenda digital
PMP	Panel Permanente para la Supervisión de la Seguridad de la Información (*Permanent Monitoring Panel of Information Security* (WFS))
SCADA	Control de supervisión y adquisición de datos
SOA	Arquitectura orientada al servicio
TCP	Protocolo de control de transmisión
NU	Naciones Unidas
CNUPDJP	Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal
UNESCO	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
ONUDD	Oficina de las Naciones Unidas contra la Droga y el Delito
URL	Localizador uniforme de recursos
WFS	Federación Mundial de Científicos (*World Federation of Scientists*)
CMSI	Cumbre Mundial sobre la Sociedad de la Información

Acerca de la Unión Internacional de Telecomunicaciones y la Agenda sobre Ciberseguridad Global

La Unión Internacional de Telecomunicaciones (UIT) es la organización más importante de las Naciones Unidas en lo que concierne a las cuestiones relativas a la tecnología de la información y la comunicación y a la coordinación entre los gobiernos y el sector privado para el desarrollo de redes y servicios.

Tras la celebración de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) y de la Conferencia de Plenipotenciarios de la UIT de 2006, una de las principales funciones de la UIT ha pasado a ser la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación (TIC). Los Jefes de Estado y de Gobierno y otros líderes mundiales que participaron en la CMSI, al igual que los Estados Miembros de la UIT, confiaron a esta organización la tarea de adoptar medidas concretas para vencer las amenazas e incertidumbres relacionadas con la sociedad de la información. A fin de llevar a bien su mandato, el Dr. Hamadoun I. Touré, Secretario General de la UIT, puso en marcha en 2007 el marco internacional de cooperación conocido como Agenda sobre Ciberseguridad Global (ACG).

La ACG tiene como objetivo aumentar la confianza y la seguridad en la sociedad de la información. Esta Agenda está diseñada para lograr una mayor cooperación y eficacia, promoviendo la colaboración entre todos los interesados y basándose en las iniciativas en curso para evitar la duplicación de esfuerzos. La ACG es la primera alianza verdaderamente multipartita a escala mundial entre el sector público y el sector privado contra las ciberamenazas. En 2008, la UIT y la Alianza Internacional Multilateral contra las Ciberamenazas (IMPACT) concluyeron formalmente un Memorándum de Entendimiento, en virtud del cual la modernísima sede de IMPACT en Cyberjaya (Malasia) pasó a convertirse en la sede física de la ACG. IMPACT es una iniciativa público-privada dedicada a desarrollar la capacidad de las comunidades de todo el mundo para prevenir las ciberamenazas, defenderse contra ellas y responder a las mismas. Desde su lanzamiento, la ACG se ha granjeado el apoyo y reconocimiento de líderes y expertos en ciberseguridad de todo el mundo. Los Padrinos de la ACG son el Excmo. Sr. Óscar Arias Sánchez, ex-Presidente de la República de Costa Rica y ganador del Premio Nobel de la Paz, y el Excmo. Sr. Blaise Compaoré, Presidente de Burkina Faso.

La ACG ha dado pie a iniciativas como la Protección de la Infancia en Línea (PIeL), la Pasarela de Ciberseguridad y, gracias a su asociación con IMPACT y al apoyo de los más importantes líderes mundiales, está implantando en la actualidad soluciones de ciberseguridad en países de todo el mundo.

Acerca de la Federación Mundial de Científicos y su Panel Permanente para la Supervisión de la Seguridad de la Información

La Federación Mundial de Científicos (WFS) fue creada en Erice, Sicilia, en 1973, por un grupo de eminentes científicos encabezados por Isidor Isaac Rabi y Antonino Zichichi. Desde entonces, otros muchos científicos se han afiliado a la Federación y entre ellos se cuentan T.D. Lee, Laura Fermi, Eugene Wigner, Paul Dirac y Piotr Kapitza.

La WFS es una asociación libre que reúne en la actualidad a más de 10 000 científicos de 110 países. Todos los miembros comparten los mismos objetivos e ideales y contribuyen voluntariamente a la promoción de los principios de la Federación. La Federación fomenta la colaboración entre científicos e investigadores de todo el mundo -el Norte, el Sur, Oriente y Occidente. La Federación y sus miembros persiguen un ideal de libre intercambio de información, de modo que los descubrimientos y avances científicos dejen de estar sólo al alcance de unos pocos. El objetivo es compartir los conocimientos con los pueblos de todas las naciones, de manera que todo el mundo pueda beneficiarse del progreso científico.

La creación de la Federación Mundial de Científicos se debe en gran parte a la existencia de un centro para la cultura científica que lleva el nombre del físico Ettore Majorana, la *Ettore Majorana Foundation and Centre for Scientific Culture* (el Centro), cuya sede se encuentra en Erice. Este Centro, que también se conoce como "Universidad del Tercer Milenio", se ha convertido en una potencia educativa a escala mundial. Desde su fundación en 1963, el Centro ha organizado 123 escuelas y 1 497 cursos para 103 484 participantes (de los cuales 125 son Premios Nobel), procedentes de 932 universidades y laboratorios de 140 países.

El Centro Ettore Majorana fue el precursor de la Federación Mundial de Científicos y sus actividades para hacer frente a las emergencias planetarias.

La Federación Mundial de Científicos identificó rápidamente 15 clases de emergencias planetarias y empezó a organizar la lucha contra estas amenazas. Uno de sus mayores logros fue la redacción en 1982 de la Declaración de Erice, elaborada por Paul Dirac, Piotr Kapitza y Antonino Zichichi, en la que se establecen claramente los ideales de la Federación y se presenta una serie de propuestas para su puesta en práctica. Otro hito en la historia de la Federación fue la celebración de una serie de Seminarios Internacionales sobre la Guerra Nuclear, que han resultado de gran eficacia para la

reducción del peligro de catástrofe nuclear a escala planetaria y que contribuyeron en último término a poner fin a la Guerra Fría. En 1986, por iniciativa de un grupo de eminentes científicos (la mayoría de los cuales eran miembros de la WFS) se fundó en Ginebra el Centro Internacional para la Cultura Científica ICSC-World Laboratory con el objetivo de contribuir a lograr los objetivos de la Declaración de Erice.

En 2001, la WFS creó su Panel Permanente para la Supervisión (PMP) de la Seguridad de la Información. Su Informe *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar* ("Hacia un orden universal en el ciberespacio: Gestión de las amenazas, desde el ciberdelito hasta la ciberguerra") fue uno de los documentos más importantes presentados por la sociedad civil a la Cumbre de Mundial sobre la Sociedad de la Información (CMSI) de las Naciones Unidas, que se celebró por primera vez en Ginebra en 2003. El PMP ha publicado numerosos artículos sobre ciberseguridad y armamento cibernético y hace presentaciones periódicas ante las sesiones plenarias de la WFS, que se celebran cada mes de agosto en Erice, de los problemas que rodean a la seguridad de la información como tema de emergencia planetaria crítica. En agosto de 2009, el PMP se mostró tan alarmado ante el potencial del armamento cibernético para poner en jaque a la sociedad y causar daños y sufrimientos innecesarios que elaboró la **Declaración de Erice sobre los principios de paz y estabilidad en el ciberespacio**, adoptada por la Plenaria de la WFS con ocasión de la 42ª Sesión de Seminarios Internacionales sobre Emergencias Planetarias, celebrada en Erice el 20 de agosto de 2009. La Declaración ha sido distribuida a todos los Estados Miembros de las Naciones Unidas.

El PMP está copresidido por el Sr. Henning Wegener, Embajador de Berlín y Madrid, y la Dra. Jody R. Westby, Directora Ejecutiva de Global Cyber Risk LLC, en Washington, DC. Han contribuido a la elaboración del presente documento los siguientes miembros del PMP:

AUTORES MIEMBROS DEL PMP

William Barletta

El Sr. William A. Barletta es Director Ejecutivo de la United States Particle Accelerator School. Es Profesor Adjunto de Física en el Massachusetts Institute of Technology y en la Universidad de California en Los Ángeles. También es Profesor Invitado de Economía en la Universidad de Ljubljana, Eslovenia, donde imparte cursos de gestión, además de Asesor del Presidente de Sincrotrone Trieste, Italia. Pertenece a la American Physical Society, donde forma parte del Grupo de Asuntos Públicos, y es Vicepresidente del Foro de Física Internacional y Vicepresidente de la División de Física de los Haces. Es

coautor y editor de cinco libros y autor de más de 150 artículos sobre una amplia gama de temas tecnológicos. barletta@mit.edu

Vladimir Britkov

El Dr. Vladimir B. Britkov es Jefe del Laboratorio de Modelización de la Información del Instituto de Análisis de Sistemas de la Academia Rusa de Ciencias en Moscú (Federación de Rusia). Es Profesor Adjunto de Análisis de Sistemas y Modelización de Sistemas en el Instituto de Física y Tecnología de Moscú (Universidad estatal). Sus campos de investigación incluyen la modelización y simulación informáticas y la aplicación de sistemas del conocimiento para la toma de decisiones. Ha sido miembro de la Junta de Directores de The International Emergency Management Society (TIEMS). Es miembro del consejo editorial de diversas publicaciones científicas dedicadas a la modelización y la simulación, y participa en varios grupos de trabajo internacionales. Forma parte del PMP de la Federación Mundial de Científicos desde 2003. britkov@gmail.com

Jacques Bus

El Sr. Jacques Bus es consultor independiente de *Digitrust.EU* en el ámbito de la Confianza y Seguridad en las Tecnologías de la Información y la Comunicación (TIC) e Investigador de la Universidad de Luxemburgo. Tras 12 años de investigación en el campo de las matemáticas, se ha dedicado a la gestión de la investigación y ha trabajado durante más de 20 años en el Programa de Investigación de las TIC de la Unión Europea. Desde hace seis años asume la Jefatura de la Unidad de *Confianza y Seguridad en las TIC*. Es miembro del PMP de la Federación Mundial de Científicos. Sus publicaciones y conferencias están dedicadas a la confianza, la seguridad, la privacidad y la gestión de la identidad. http://www.digitrust.eu

Axel Lehmann

El Sr. Axel Lehmann es Profesor Titular del Departamento de Informática de la Universität der Bundeswehr de Munich, donde ocupa la Cátedra de Modelización y Simulación. También es Presidente del Instituto de Sistemas Inteligentes (ITIS) de la Universidad. Sus principales campos de investigación van de la modelización y simulación informáticas y la aplicación de sistemas de conocimiento para el diagnóstico y la toma de decisiones, al diseño de arquitecturas informáticas innovadoras. Fue Presidente de la Sociedad Internacional de Modelización y Simulación, y miembro de la Sociedad Alemana de Informática y de diversos consejos editoriales de publicaciones científicas dedicadas a la modelización y la simulación, así como de varios grupos de trabajo y comités de evaluación internacionales, por

ejemplo, de la Unión Europea. Es miembro del PMP de la WFS desde 2001. axel.lehmann@unibw.de

Hamadoun I. Touré

El Dr. Hamadoun I. Touré, Secretario General de la Unión Internacional de Telecomunicaciones (UIT) desde enero de 2007, fue reelegido para un segundo mandato por la Conferencia de Plenipotenciarios de la UIT, celebrada en Guadalajara (México) en octubre de 2010. Entre 1998 y 2006 fue Director de la Oficina de Desarrollo de las Telecomunicaciones (BDT) de la UIT y posee una amplia experiencia profesional tanto en el sector público como en el sector privado. Nacido en 1953, el Dr. Touré posee un Máster en Ingeniería Eléctrica del Instituto Técnico de Electrónica y Telecomunicaciones de Leningrado (LEIS, URSS) y es Doctor por la Universidad de Electrónica, Telecomunicaciones e Informática de Moscú (MTUCI, Federación de Rusia). Su meta es hacer de la UIT una organización innovadora y orientada al futuro, adaptada para responder a los retos que conllevan los rápidos cambios del entorno de las TIC, y seguir al frente de la Unión para llevar a la práctica las resoluciones de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) y alcanzar los Objetivos de Desarrollo del Milenio (ODM). hamadoun.toure@itu.int

Vitali Tsygichko

El Dr. V.N. Tsygichko, Coronel jubilado del Ejército Ruso, es miembro de pleno derecho de la Academia Rusa de Ciencias Naturales y, desde 1985, Investigador Jefe del Instituto de Análisis de sistemas de la Academia Rusa de Ciencias (ISA RAS). En la actualidad trabaja como experto en problemas de seguridad de la información para el Ministerio de Asuntos Exteriores de la Federación de Rusia. Desde 1967 participa en las simulaciones matemáticas de operaciones militares del Instituto Central de Investigación del Ministerio de Defensa. Entre 1988 y 1991 dirigió un Centro de Investigación de Problemas de Seguridad Nacional de carácter independiente. Los intereses científicos del Dr. Tsygichko van de los problemas metodológicos y sistémicos de la modelización de procesos socioeconómicos a la teoría de la decisión, pasando por el análisis de sistemas aplicados, la teoría y práctica de la previsión socioeconómica, la garantía de la seguridad nacional y la estabilidad estratégica, los problemas de seguridad de la información y los problemas geopolíticos. Es autor de más de 200 artículos y ocho libros. Es colaborador permanente de publicaciones como Military Thought, Military Bulletin, Independent Military Review, y toda una serie de publicaciones extranjeras. Se graduó en la Escuela Militar de Artillería de Ryazan y la Academia Militar Dzerzhinsky, y es Doctor en ciencias (Ingeniería) y Profesor. vtsygichko@inbox.ru

Henning Wegener

El Sr. Henning Wegener fue Embajador de Alemania. Ha ocupado los cargos de Embajador para el Desarme en Ginebra (1981-1986), Secretario General Adjunto de Asuntos Políticos de la OTAN (1986-1991) y Embajador en España. El Embajador Wegener fue primero Presidente (2001-2009), y ahora Vicepresidente del PMP de la Federación Mundial de Científicos. Su trabajo ha quedado reflejado en diversas publicaciones dedicadas a la política exterior y de seguridad, incluida la ciberseguridad. Entre otros títulos, el Sr. Wegener ostenta el de Doctor en Ciencias Jurídicas por la Yale Law School. henningwegener@hotmail.com

Jody R. Westby

La Sra. Jody R. Westby es Directora Ejecutiva de Global Cyber Risk LLC, Washington, DC, y es Miembro Adjunta Distinguida del Carnegie Mellon CyLab. La Sra. Westby presta servicios jurídicos y de consultoría a clientes de los sectores público y privado de todo el mundo en las esferas de privacidad, seguridad, ciberdelincuencia, protección de las infraestructuras esenciales y espionaje económico. Preside el Comité de Privacidad y Delitos Informáticos (Sección de Leyes de Ciencia y Tecnología) del Colegio de Abogados de América (American Bar Association's (ABA)) y es su representante ante la Conferencia Nacional de Juristas y Científicos. La Sra. Westby fue miembro del Grupo de Expertos de Alto Nivel del Secretario General de la UIT y lideró la elaboración de la obra *ITU Toolkit for Cybercrime Legislation* (Colección de herramientas de la UIT para la legislación en materia de ciberdelitos). Es copresidenta del PMP de la Federación Mundial de Científicos. La Sra. Westby es coautora y editora de cuatro libros sobre ciberdelincuencia internacional, ciberseguridad y privacidad, y ha publicado numerosos artículos. Interviene en conferencias sobre estos temas en todo el mundo. westby@globalcyberrisk.com

Preámbulo

En el mundo de 2011, disfrutamos de los beneficios de una sociedad mundial de la información sin fronteras, pero éstos también entrañan la amenaza de los ciberataques. Éstos pueden producirse en cualquier momento y lugar, y ocasionar daños inmensos en cuestión de segundos. Con la creciente articulación de las tecnologías de la información y la comunicación (TIC) y las infraestructuras nacionales esenciales, este potencial nefasto crece de manera exponencial.

Para frenar esta creciente amenaza hemos de actuar ahora.

En la Cumbre Mundial sobre la Sociedad de la Información (CMSI), los líderes de la industria y los gobiernos asignaron a la Unión Internacional de Telecomunicaciones (UIT) la tarea de coordinar un mecanismo de creación de confianza y seguridad en la utilización de las TIC. A partir de entonces, su Secretario General, el Dr. Touré, ha presentado la Agenda sobre ciberseguridad Global (ACG), y la UIT se ha empeñado en el cumplimiento de este mandato a través de una serie de iniciativas. Por encima de todo, la UIT sigue hondamente preocupada por las ciberamenazas de que son objeto sus Estados Miembros.

La Federación Mundial de Científicos (WFS) fomenta la colaboración entre científicos e investigadores de todo el mundo. Su objetivo es alcanzar el libre intercambio de información, de manera que todo el mundo pueda beneficiarse del progreso científico. En 2009, el Panel Permanente para la Supervisión (PMP) de la Seguridad de la Información de la WFS elaboró la Declaración de Erice sobre los principios de paz y estabilidad en el ciberespacio, que adoptó la Plenaria de la WFS con ocasión de la 42ª Sesión del Seminario Internacional sobre Emergencias Planetarias, celebrada en Erice (Sicilia) el 20 de agosto de 2009.

A fin de alcanzar el objetivo común de lograr la paz en el ciberespacio, es fundamental que colaboren la UIT y los miembros de la comunidad científica y tecnológica. En la práctica no podremos contrarrestar eficazmente la amenaza de guerra cibernética sin

contar con el conocimiento que poseen los expertos acerca de las tecnologías que están cambiando el panorama mundial.

Esta publicación da voz a la comunidad científica y es un paso necesario en el proceso de instauración de una cooperación internacional para superar esos problemas. Agradecemos la oportunidad que se nos brinda de presentar nuestra opinión sobre este tema esencial.

Dr. Hamadoun I. Touré
Secretario General
Unión Internacional de Telecomunicaciones

Profesor Dr. Antonino Zichichi
Presidente
Federación Mundial de Científicos

1 Introducción

Por Jody R. Westby

Esta publicación tiene como finalidad promover el concepto de paz mundial en el ciberespacio, o ciberpaz, por medio de:

- un examen del alcance de las TIC como soporte de la vida diaria;
- una evaluación de las ciberamenazas actuales y de su evolución;
- un análisis de las repercusiones del ciberdelito y del conflicto cibernético;
- una evaluación de la validez de los marcos jurídicos en vigor;
- una definición del concepto de ciberpaz, y su establecimiento como principio orientador primordial para un comportamiento pacífico en el ciberespacio; y
- el trazado de un itinerario para el futuro.

La Internet es el sistema nervioso central de la sociedad. Hay que tener presente que todos los sectores de infraestructuras esenciales dependen de las TIC. Su gestión está a cargo de unos sistemas de Control de supervisión y adquisición de datos (SCADA) y otros procesos complejos de tecnología de la información (TI) que están conectados de alguno u otro modo a Internet. Por ejemplo, los hospitales y centros médicos utilizan las TIC para todo, desde la resolución de las urgencias hasta los sistemas de soporte vital. Los sectores del petróleo y el gas y del transporte implantan sistemas sofisticados de procesamiento y navegación que están totalmente informatizados, y las empresas financieras desarrollan su actividad a través de sistemas de pago y procesamiento electrónico. Los gobiernos dependen de las TIC para prestar servicios, gestionar operaciones en distintas zonas geográficas, mantener la seguridad pública y proteger sus territorios. Las empresas dependen de sistemas informáticos que gestionan las cadenas de suministro, las relaciones con los clientes y los flujos financieros, y que cumplen funciones de fabricación. Y los sistemas de comunicaciones y redes de servicios públicos son las infraestructuras "superesenciales" de las que dependen todas las demás.

En la actualidad, Internet también se ha integrado completamente en las tareas cotidianas y la vida de las personas. Ya sea en el trabajo, el aprendizaje o el ocio, las TIC desempeñan un papel. Internet permite una divulgación de los conocimientos y la información sin precedentes en la historia. Las redes sociales permiten establecer vínculos entre las poblaciones e influyen sobre las mismas, con total independencia y de manera imprevista para sus gobiernos. Internet ha hecho posible una mayor autonomía de la persona, la expansión del ser humano y la difusión de ideas peculiares

a través de un mecanismo que desconoce en gran medida las fronteras y las consideraciones diplomáticas o políticas. En la actualidad, gracias a su capacidad para crear contenidos y distribuirlos a escala mundial, el individuo puede influir con rapidez sobre percepciones, valores, ideas y prejuicios.

Sin embargo, la omnipresencia de Internet también ha dado lugar a la aparición de actividades criminales y ha creado nuevas vías para la recopilación de información sensible y para el conflicto. Las vulnerabilidades inherentes a los sistemas operativos, programas informáticos y ajustes de seguridad hacen posible intervenciones que amenazan los servicios básicos a la población civil, facilitan el espionaje económico y afectan a las actividades gubernamentales. Los virus, gusanos, ataques de denegación de servicio distribuido (DDoS), robos de datos privados, correos basura y fraudes socavan la fiabilidad de las TIC y la capacidad de funcionamiento de las sociedades y economías.

Programas de seguridad eficaces permitirán mejorar la resistencia de los sistemas y contribuirán a detectar, prevenir y mitigar este tipo de acciones. Los ajustes tecnológicos y las innovaciones contribuirán a bloquear y rastrear los ataques, y la armonización de la legislación en materia de ciberdelito permitirá avanzar en la investigación y persecución de los ciberdelincuentes. Es mucho lo que hay que hacer en cada una de estas áreas, pero el problema de mayor envergadura y potencial destructor se plantea cuando los Estados-nación emplean estas tácticas para iniciar un ciberconflicto.[1] Ya existen numerosos ejemplos de la manera en que los conflictos políticos y militares se extienden al ciberespacio, socavando eficazmente la confianza en las TIC y causando una exposición a graves riesgos. En los siguientes capítulos de esta publicación se describen varios ejemplos.

Hasta la aparición de la sociedad de la información, el poder y el liderazgo recaían habitualmente en quienes disponían de autoridad política, superioridad militar y dominio económico. Los Estados-nación y las organizaciones internacionales dictaban las normas y los valores sociales, y el conflicto armado se regía por leyes y tratados basados en la integridad territorial y las capacidades defensivas por tierra, mar y aire. En la actualidad, sin embargo, Internet ha supuesto una alteración radical de este equilibrio de poderes. Nada mejor para ilustrar esta afirmación que la propia historia de Internet.

Los acontecimientos mundiales pueden suponer una importante motivación. Al salir de la Segunda Guerra Mundial, los Estados Unidos se enfrentaban a un nuevo tipo de

---

1 El término "ciberconflicto" incluye escenarios que cabe calificar como "guerra cibernética".

enemigos: la Guerra Fría, el comunismo y las amenazas de ataque nuclear. Para responder a la inquietud suscitada por la supremacía científica de los soviéticos tras el lanzamiento del Sputnik, el primer satélite artificial, el Presidente Eisenhower fundó la Agencia de Proyectos de Investigación Avanzada (ARPA), hoy DARPA, a fin de coordinar todas las investigaciones tecnológicas estadounidenses.[2] Se contrató a J.C.R. Licklider, del Massachusetts Institute of Technology (MIT), para ponerle al frente del programa de investigación informática de la ARPA. Unos meses antes, había publicado una serie de memorandos en los que se trataba de una "red galáctica" de computadoras interconectadas que hacían posible el acceso compartido a programas y archivos. Vint Cerf, Bob Kahn, y algunos de los demás "padres de Internet" observaron posteriormente que, "en su espíritu, el concepto era muy similar al de la Internet actual".[3]

Más o menos al mismo tiempo, la Fuerza Aérea, preocupada por su capacidad para mantener las operaciones de mando y control tras un ataque nuclear, encargó un estudio al grupo RAND sobre una red militar capaz de sobrevivir a tal ataque y proporcionar "comunicaciones mínimas esenciales".[4] La labor del grupo RAND (1962–1965) concluyó con un informe de Paul Baran, en el que se describía la manera en que podía proporcionarse esa capacidad a través de redes de computadoras con conmutación de paquetes.[5] Al mismo tiempo (y sin saberlo el grupo RAND), tres ingenieros del MIT estaban discutiendo el concepto de las computadoras en red y de la conmutación de paquetes.[6] A finales de 1966, uno de los ingenieros del MIT,

---

2 "A Brief History of the Net", *Fortune*, 9 de octubre de 2000, pág. 34, http://money.cnn.com/magazines/fortune/fortune_archive/2000/10/09/289297/index.htm (en adelante "Fortune"); *véase también* Dave Krisula, "The History of the Internet," agosto de 2001 (edición de 2009 ampliada), www.davesite.com/webstation/net-history1.shtml (en adelante "Krisula").

3 Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts, Stephen Wolff, "A Brief History of the Internet," Internet Society (ISOC) todo sobre Internet, www.isoc.org/internet/history/brief.shtml (en adelante "A Brief History of the Internet"); Licklider público su serie de memorandos sobre la "red galáctica" en agosto de 1962, y comenzó a trabajar en la ARPA en octubre de 1962.

4 Krisula; *véase también* Fortune; Stewart Brand, "Founding Father", *Wired*, marzo de 2001, Pág. 148, www.wired.com/wired/archive/9.03/baran_pr.html (en adelante "Brand").

5 Brand, Págs. 145-153; *véase también* Krisula.

6 A Brief History of the Internet; *véase también* Brand, Pág. 146; Krisula.

Lawrence Roberts, se marchó a la DARPA "para desarrollar el concepto de la red de computadoras".[7]

El resto de la historia es sobradamente conocido. En 1971, la ARPANET, que es como se llamó primero a Internet, contaba con 23 computadoras centrales que conectaban a centros de investigación gubernamentales y universidades de todos los Estados Unidos. Desde 1981 pasó a llamarse Internet y, a partir de 1991, nació la World Wide Web, desarrollada en el Centro Europeo para la Investigación Nuclear (CERN) por Sir Timothy Berners-Lee.[8] De la combinación de Internet y la web nacieron ideas de utilización comercial, pero las empresas no tenían acceso a la red medular a partir de la NSFNET de la National Science Foundation (NSF).

En 1995, la NSF dio su acuerdo y cedió la gestión del acceso a la red medular de Internet a cuatro empresas comerciales, de modo que, en 1996 estaban en línea cerca de 10 millones de computadoras centrales e Internet se extendía a todo el planeta. En el plazo de 30 años, Internet pasó de ser "un concepto de la Guerra Fría para controlar los restos destrozados de una sociedad postnuclear, a ser la superautopista de la información".[9] La combinación entre Internet y la World Wide Web ha penetrado todas las capas de las economías y las sociedades, y ha creado una transformación social que era impensable 20 años atrás. Hoy en día hay cerca de 2 000 millones de usuarios en línea, y no existen fronteras geográficas para Internet. En la actualidad, la gestión de Internet conlleva cuestiones tanto técnicas como de políticas públicas, que implican a todas las partes interesadas y a las organizaciones intergubernamentales e internacionales pertinentes.

Lo irónico es que este invento de la época de la Guerra Fría, en combinación con la internacionalización de la ciencia que dio lugar a la web, supone hoy uno de los mayores retos para la paz mundial. Aunque, al analizar los intereses de la seguridad y la economía nacional, aún debe concederse gran importancia a los factores

---

7 A Brief History of the Internet.

8 Elizabeth D. Hoover, "The Inventor of the World Wide Web", *AmericanHeritage.com*, 12 de noviembre de 2005, www.americanheritage.com/articles/web/20051112-internet-world-wide-web-tim-berners-lee-computer-geneva-cern-enquire-html-url-world-wide-web-consortium.shtml.

9 "Life on the Internet: Net Timeline," PBS, www.pbs.org/opb/nerds2.0.1/timeline/; *véase también* Krisula.

geopolíticos[10], Internet ha trastornado el análisis tradicional de la política exterior. Las dimensiones geocibernéticas influyen cada vez más en la conducta de los Estados-nación, y los bloques geopolíticos están forzando la aparición de un nuevo paradigma.

Ya no se trata de que los Estados Unidos mantengan "comunicaciones esenciales mínimas": ahora se trata de saber cómo pueden todos los países del mundo mantener la estabilidad geocibernética y asegurarse de que sus infraestructuras esenciales no puedan utilizarse como arma contra civiles inocentes e indefensos, resultando en un sufrimiento y una destrucción innecesarios.

El autor define el término "geocibernética" como la relación entre Internet y la geografía, demografía, economía y política de una nación y su política exterior. La "estabilidad geocibernética" se define como la capacidad de todos los países de utilizar Internet para su beneficio económico, político y demográfico, absteniéndose al mismo tiempo de cualquier actividad que pudiera causar un sufrimiento y una destrucción innecesarios.[11]

En la actualidad, el mundo entero se enfrenta a nuevas amenazas surgidas de Internet, y ya no existe certeza en cuanto a la capacidad de cualquier Estado-nación para mantener a salvo sus comunicaciones, líneas de mando, control y capacidades informáticas (C4) frente a los ataques terroristas, las bandas de criminales organizados y otros Estados-nación. Para los países, las TIC plantean desafíos hasta ahora desconocidos para la seguridad nacional y económica. Hoy los individuos son capaces de eludir a la autoridad y realizar ataques asimétricos que pueden paralizar toda una infraestructura e interrumpir las comunicaciones, y ahora los sistemas más débiles pueden amenazar la seguridad de la mayor de las naciones.

---

10 La geopolítica se define como "1) el estudio de las relaciones entre la política y la geografía, la demografía y la economía, especialmente en lo que respecta a la política exterior de una nación; 2) a. una política gubernamental que emplee la geopolítica; b. una doctrina nazi que mantiene que las necesidades geográficas, económicas y políticas de Alemania justifican su invasión y ocupación de otros países; 3) una combinación de factores geográficos y políticos que se relacionan con una nación o región o influyen en ella". American Heritage Dictionary, 2000, www.dictionary.com/search?q=geo-political.

11 Presentada inicialmente ante la Conferencia del ANSER Institute of Homeland Security Conference, "Homeland Security 2005: Charting the Path Ahead", Universidad de Maryland, Presentación a cargo de Jody Westby, "A Shift in Geo-Cyber Stability and Security", 6-7 de mayo de 2002.

El ciberconflicto puede entrañar una amenaza para la vida cuando afecta a infraestructuras informáticas esenciales. También puede dar lugar a operaciones de información que vulneran los derechos humanos internacionalmente reconocidos, provocan violencia y causan graves daños económicos. El riesgo para las personas y los Estados-nación es enorme -y está desvinculado de los marcos jurídicos en vigor que aún no se han adaptado adecuadamente a la era cibernética.

Se trata de una necesidad urgente. La rapidez con la que los países están desarrollando las líneas de mando cibernéticas y ampliando sus capacidades militares para incluir el ciberconflicto debe compensarse a través de un acuerdo entre los Estados-nación por el que éstos reconozcan un nuevo nivel de "comunicaciones mínimas esenciales" que ha de protegerse frente a cualquier conflicto. Una acción de este tipo evitará la destrucción y el sufrimiento innecesarios de quienes se vean implicados en un conflicto, y evitará daños a terceros países no implicados. Este nivel de geociberestabilidad resulta vital para evitar que se pierdan los beneficios de Internet como consecuencia de las fuerzas destructoras de la tecnología.

Las organizaciones plurinacionales son el punto de partida más evidente. Tienen que comenzar definiendo el nivel de estabilidad mínimo de las infraestructuras y las comunicaciones que se requiere para proteger a los civiles inocentes y preservar las funciones sociales básicas, y asegurándolo a través de un acuerdo diplomático y del imperio de la ley. Esto requerirá la contribución de muy diversas partes interesadas, entre las que figuran los individuos, la industria, la sociedad civil, los sectores académicos, las fiscalías, los expertos políticos, los servicios de auxilio y las fuerzas del orden. De esta manera, las TIC e Internet podrán proporcionar un marco internacional positivo para la colaboración entre los países, y lograr una mejor comprensión y aceptación de los distintos valores culturales y sociales en todo el mundo.

Esta obra se inspira en el concepto de ciberpaz como principio orientador para el comportamiento en el ciberespacio. En consecuencia, la ciberpaz debería ser un objetivo que persiguieran todas las naciones. Las ventajas de la ciberpaz superan con mucho las consecuencias destructoras del ciberconflicto.

Esta publicación, de la que son coautores Hamadoun I. Touré, Secretario General de la Unión Internacional de Telecomunicaciones, y diversos miembros del Panel Permanente para la Supervisión de la Seguridad de la Información de la Federación Mundial de Científicos, pretende servir como un llamamiento para que todas las partes interesadas garanticen un nivel de estabilidad mínimo en Internet y sus infraestructuras y promuevan el concepto de la ciberpaz mundial.

2 El ciberespacio y la amenaza de guerra cibernética

Por Hamadoun I. Touré

Las tecnologías de la información y la comunicación (TIC) se han convertido en una parte integrante de la vida cotidiana de muchas personas de nuestro planeta. Las comunicaciones, las redes y los sistemas digitales proporcionan a la comunidad mundial los recursos esenciales y la infraestructura indispensable sin los cuales muchas poblaciones no podrían florecer ni sobrevivir. Estas estructuras y sistemas representan un nuevo ámbito, que conlleva nuevos desafíos para preservar la paz y la estabilidad. Si no se dispone de los mecanismos necesarios para mantener la paz, las ciudades y las comunidades del mundo se verán expuestas a ataques de una diversidad ilimitada y sin precedentes. Este tipo de ataques podrían producirse sin previo aviso. Los computadores y los teléfonos celulares dejarían súbitamente de funcionar, las pantallas de los cajeros automáticos y de los distribuidores bancarios quedarían en blanco, los sistemas de control del tráfico aéreo, ferroviario y vial quedarían fuera de servicio y reinaría el caos en las autopistas, los puentes y canales fluviales; las mercancías caducarían y quedarían abandonadas muy lejos de las poblaciones hambrientas. La caída de la red eléctrica dejaría en la oscuridad más absoluta a los hospitales, los hogares, los centros comerciales y a todas las comunidades. Las autoridades gubernamentales serían incapaces de evaluar los daños, comunicarse con el resto del mundo para informar sobre la crisis o proteger a sus vulnerables ciudadanos contra los subsiguientes ataques. Ésta sería la inextricable situación de una comunidad paralizada por la caída instantánea de todas las redes digitales. Éste es el poder devastador de un nuevo tipo de guerra: "la guerra cibernética".

Un nuevo dominio: ciberespacio, seguridad y guerra

La amenaza de una guerra cibernética nunca ha tenido tanta importancia como ahora. Hoy en día, los adelantos tecnológicos y la creciente infraestructura digital han hecho que poblaciones enteras dependan de sistemas entrelazados y complejos. La demanda de Internet y de conectividad digital exige una integración cada vez mayor de las TIC en productos que anteriormente funcionaban sin estas tecnologías, por ejemplo automóviles, edificios e incluso sistemas de control para las redes de distribución eléctrica y de transporte. Prácticamente todos los servicios modernos dependen de la utilización de las TIC y de la estabilidad del ciberespacio, ya se trate del suministro eléctrico, los sistemas de transporte, los servicios militares, la logística, etc. El "ciberespacio" es un ámbito físico y conceptual en el que existen todos estos sistemas. Por consiguiente, el significado general de "guerra cibernética" es una guerra que se

lucha en el ciberespacio y donde las TIC son a su vez las armas y los objetivos.[12] El rápido aumento de la dependencia respecto de las redes inteligentes y otros sistemas de control y supervisión basados en Internet, hace que los recursos de energía, transporte y defensa hayan quedado expuestos a los ataques de quienes desean causar estragos a los gobiernos y la población civil.[13] Así pues, el aumento de la ciberseguridad y la protección de la infraestructura esencial de la información son dos aspectos fundamentales para la seguridad y la economía de cualquier país.

A medida que aumenta la dependencia respecto de las TIC en el plano mundial, también aumenta la vulnerabilidad a los ataques contra las infraestructuras esenciales a través del ciberespacio. Aunque las fronteras exactas de una "guerra cibernética" aún no están bien definidas, los considerables ataques contra la infraestructura de la información y los servicios de Internet que se han producido en la última década dan una idea de la posible forma y alcance de un conflicto en el ciberespacio. Los ataques producidos en Georgia[14], Estonia[15], Corea del Sur y Estados Unidos[16] se han asociado a una guerra cibernética. En Brasil, varios apagones se han relacionado con ciberataques y, en 2008 los piratas informáticos consiguieron entrar y tomar el control del sitio web

---

12 Steven Elliot, "Analysis on Defense and Cyberwarfare", *Infosec Island*, 8 de julio de 2010, https://infosecisland.com/blogview/5160-Analysis-on-Defense-and-Cyber-Warfare.html (hereinafter "Elliot").

13 Ellen Messmer, "Cyberattack Seen as Top Threat to Zap U.S. Power Grid", *NetworkWorld*, 2 de junio de 2010, http://www.networkworld.com/news/2010/060210-nerc-cyberattack-power-grid.html (informa de que la amenaza de un ciberataque coordinado, que puede combinarse con un ataque físico, se considera la amenaza más apremiante "de elevado impacto y baja frecuencia" para la red de suministro eléctrico de Norteamérica) (en adelante, "Messmer").

14 Thomas Claburn, "Under Cyberattack, Georgia Finds 'Bullet-Proof' Hosting With Google And Elsewhere," *InformationWeek*, 12 de agosto de 2008, www.informationweek.com/news/security/attacks/showArticle.jhtml?articleID=210002702.

15 Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, 21 de agosto de 2007, www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

16 Choe Sang-Hun and John Markoff, "Cyber attacks Jam Government and Commercial Web Sites in U.S. and South Korea," *The New York Times*, 8 de Julio de 2009, www.nytimes.com/2009/07/09/technology/09cyber.html; Jack Date, Jason Ryan, Richard Sergay, and Theresa Cook, "Hackers Launch Cyberattack on Federal Labs," *ABC News*, 7 de diciembre de 2007, http://abcnews.go.com/TheLaw/Technology/story?id=3966047&page=1.

del Gobierno durante una semana.[17] Estos apagones en Brasil ilustran la posible magnitud de estos nuevos tipos de ciberataques: los informes se parecen a una escena de una película de ciencia ficción, dado que quedaron totalmente paralizados los trenes del metro, los semáforos e incluso la segunda central hidroeléctrica más grande del mundo, la presa *Itaipu,* y se vieron afectadas más de 60 millones de personas.[18]

La guerra cibernética también puede afectar al sector privado. Gigantes de servicios web tales como *Google*[19] and *Twitter*[20] sufrieron ataques en 2009 y mucho antes, en el año 2000, se lanzaron ataques de denegación del servicio contra empresas muy conocidas tales como la *CNN, eBay* y *Amazon*[21] que interrumpieron algunos servicios durante varias horas e incluso días. Los piratas informáticos también han lanzado ataques contra los sistemas de control de aeropuertos y han llegado a desactivar equipos esenciales tales como los servicios telefónicos y las luces de pista.[22] Según los datos, más de seis países han sido víctimas de ciberataques en los últimos tres años y en sólo los primeros meses de 2010 sufrieron ataques al menos 34 empresas privadas.[23] Aunque estos problemas de seguridad son graves, todavía no es demasiado tarde para evitar los posibles efectos catastróficos mediante la creación de productos más seguros y adopción de prácticas y normas de seguridad en el marco de una

---

17 Michael Mylrea. "Brazil's Next Battlefield: Cyberspace," *Foreign Policy Journal*, 15 de noviembre de 2009, http://foreignpolicyjournal.com/2009/11/15/brazils-next-battlefield-cyberspace (hereinafter "Mylrea").

18 Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired*, 21 de agosto de 2007, www.wired.com/politics/security/magazine/15-09/ff_estonia?currentPage=all.

19 Andrew Jacobs and Miguel Helft, "Google, Citing Attack, Threatens to Exit China," *The New York Times*, 12 de enero de 2010, www.nytimes.com/2010/01/13/world/asia/13beijing.html.

20 Eliot Van Buskirk. "Denial-of-Service Attack Knocks Twitter Offline (Updated)," Wired.com, 6 de agosto de 2009, www.wired.com/epicenter/2009/08/twitter-apparently-down/.

21 *See* Abraham D. Sofaer and Seymour E. Goodman, *The Transnational Dimension of Cyber Crime and Terrorism,* 2001 at 14, http://media.hoover.org/documents/0817999825_1.pdf.

22 *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems are Under Way, but Challenges Remain*, United States Government Accountability Office, septiembre de 2007, GAO-07-1036, www.gao.gov/new.items/d071036.pdfIn 1997 (los piratas informáticos atacaron el Aoeropuerto de Worcester en Estados Unidos, y lograron desactivar los servicios telefónicos hacia la torre de control del aeropuerto y apagar el sistema de control de las luces de pista).

23 Elliot.

colaboración internacional.24 Lograr que Internet sea un lugar más seguro y proteger las TIC contra la interrupción y destrucción deben ser prioridades si queremos proteger a las poblaciones civiles, garantizar el buen funcionamiento de la infraestructura básica y velar por el desarrollo constante de nuevos servicios.

La guerra cibernética en cuanto amenaza a la infraestructura nacional

El concepto de guerra cibernética engloba no solamente los ataques contra las instalaciones y los sistemas militares, sino también contra la infraestructura esencial de la sociedad -incluidas las redes inteligentes y las redes de adquisición de datos y control (SCADA)- que garantizan el funcionamiento y la defensa de la sociedad. Aunque utilizan un medio diferente (el ciberespacio y las TIC que funcionan en el mismo), los enemigos pueden emplear armas y desencadenar un conflicto ofensivo-defensivo de manera bastante parecida a una guerra tradicional. Las tácticas de guerra cibernética suelen consistir en la recopilación de datos o la infiltración en sistemas informáticos para causar daños a los sistemas esenciales.[25] Entre las posibles armas cibernéticas cabe citar los virus y gusanos informáticos, las herramientas de recopilación de ciberdatos, las señales interferentes de comunicaciones inalámbricas, los programas informáticos falsificados y contaminados, las armas de impulsos electromagnéticos, las herramientas de reconocimiento de computadores y las redes y bombas de relojería con troyanos incorporados.

El suministro eléctrico en muchos países se ha vuelto especialmente vulnerable a los ataques al aumentar su dependencia respecto de las redes inteligentes. Las redes inteligentes son sistemas digitales que conectan los servicios públicos a una red de control central, denominada a menudo red SCADA. Las redes SCADA recaban información sobre el consumo y utilización de energía, mientras que las redes inteligentes ofrecen un canal digital para el flujo de información entre el consumidor y el proveedor.[26] Estas tecnologías se utilizan hoy en día en procesos y sistemas muy diversos, tales como: sistemas de gestión hidrológicos, conductos de gas, redes de transmisión y distribución de energía eléctrica, sistemas eólicos, sistemas de comunicación de masas, fabricación, producción, sistemas de tránsito de masas,

---

24 Joshua Pennell, "Securing the Smart Grid: The Road Ahead," at 2, *NetworkSecurityEdge.com*, 5 de febrero de 2010, www.networksecurityedge.com/content/securing-smart-grid-road-ahead.

25 Elliot.

26 "Smart Grid," U.S. Department of Energy, www.oe.energy.gov/smartgrid.htm; "SCADA," *TopBits.com*, www.tech-faq.com/scada.html (en adelante, "SCADA").

sistemas de control medioambiental, control del tráfico aéreo y de semáforos.[27] Los proveedores conectan cada vez más las redes inteligentes a Internet para permitir el acceso a distancia y ofrecer mayor funcionalidad.

La conexión de redes tiene ventajas considerables, tales como la reducción del consumo de energía y comunicaciones más rápidas entre el cliente y el proveedor. El problema es que centralizan los datos y el control de redes de alta potencia en una red que dispone de múltiples puntos de acceso. Al tener más puntos de acceso y estar más interconectados, los agresores disponen de numerosas formas para infiltrarse en la redes inteligentes y las redes SCADA.[28] Por ejemplo, un contador inteligente (un contador eléctrico conectado a la red) se puede piratear e infectar fácilmente, y luego utilizarse para propagar un gusano a otros contadores y, en última instancia, causar una sobrecarga o apagón de la red eléctrica.[29] Aunque muchas empresas tratan de proteger sus redes aislando los centros de control de las demás redes (una técnica denominada "disociación"), estos intentos de aislar totalmente ciertos componentes suelen fallar, a veces sin que se dé cuenta el administrador del sistema.[30] Las bombas lógicas son otro tipo de armas que utilizan los atacantes para interrumpir e incluso destruir una red inteligente. Los piratas se infiltran en la red para ocultar software maléfico y no activan estas bombas hasta más tarde con el fin de efectuar un ataque coordinado o para causar pequeñas interrupciones del suministro eléctrico.[31] Estas bombas crean otro problema de seguridad por cuanto pueden hacerse detonar por accidente o por un pirata distinto que las descubra más tarde.[32]

---

27 SCADA.

28 Katie Fehrenbacher, "10 Things to Know About Smart Grid Security," 9 de octubre de 2009, Earth2Tech, Gigaom, http://gigaom.com/cleantech/10-things-to-know-about-smart-grid-security/, (en adelante, "Fehrenbacher"}.

29 *Id*.

30 "SCADA Security and Terrorism: We're Not Crying Wolf," at 26, BlackHat, www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Maynor-Graham-up.pdf.

31 Siobhan Gorman. "Electricity Grid in U.S. Penetrated By Spies," *The Wall Street Journal,* 8 de abril de 2009, http://online.wsj.com/article/NA_WSJ_PUB:SB123914805204099085.html.

32 Ellen Messmer. "'Cyberwar' author: U.S. needs radical changes to protect against attacks," *NetworkWorld*, 7 Apr. 2010, www.networkworld.com/news/2010/040710-clarke-book-review.html (en adelante, "Radical Change").

Los países que han invertido en redes inteligentes aseguran que sufren intentos de ataque y de sondeo que ascienden a miles de ataques al día.[33] Según algunas estimaciones, los ciberataques constituyen la mayor amenaza a las redes nacionales de suministro eléctrico.[34] Los ataques a distancia podrían estar dirigidos contra la infraestructura física, como generadores de potencia y transformadores, y pueden ocasionar su autodestrucción.[35] Estos ataques tendrían con toda probabilidad consecuencias de gran alcance, ya que las compañías eléctricas no suelen almacenar equipos de repuesto, que son muy caros, y su fabricación y suministro podría tardar meses.[36] Además de dejar a los ciudadanos sin energía, un ataque contra la red inteligente podría causar enormes daños financieros. El precio de los generadores eléctricos puede elevarse a varios millones de dólares y la inversión general en redes eléctricas asciende a decenas de miles de millones en algunos países.[37]

Además del potencial de destrucción física masiva y las pérdidas financieras inmediatas, la amenaza de futuros ciberataques merma la confianza en las tecnologías nuevas y existentes, como las redes inteligentes y, a su vez, la fiabilidad de los recursos electrónicos, financieros y sanitarios. Esta pérdida de confianza puede causar por sí misma enormes trastornos socioeconómicos.[38] El desarrollo de redes inteligentes para reactores nucleares (e instalaciones de armas nucleares) aumenta aún más los riesgos y los posibles daños. Aparte de las estrategias de ataque y defensa tradicionales, la guerra cibernética podría consistir también en atacar los sistemas internos de un país

---

33 *Id.* (informa que la red de suministro eléctrico de Estados Unidos recibe cientos de miles de sondeos por día); Fehrenbacher (declara que los más de 40 millones de contadores inteligentes instalados globalmente han sufrido varias rupturas de seguridad).

34 Messmer.

35 Mylrea.

36 "Cyberwar: War in the fifth domain," 7 Jan. 2010, *The Economist*, www.economist.com/node/16478792 (en adelante, "Fifth Domain").

37 *Smart Grid: Hardware and Software Outlook*, Zpryme, 2009 at 2, www.zpryme.com/SmartGridInsights/2010_Smart_Grid_Hardware_Software_Outlook_Zpryme_Smart_Grid_Insights.pdf (declara que la industria de redes inteligentes de Estados Unidos fue valorada en 21 400 millones en 2009 y, según las estimaciones, alcanzará unos 42 800 millones en 2014); Jonathan Weisman and Rebecca Smith,"Obama Trumpets Energy Grants," *The Wall Street Journal*, 28 Oct. 2009, http://online.wsj.com/article/SB125663945180609871.html (en el que se informa que el Presidente Obama ha anunciado un plan de estímulo de 3.400 millones USD para proyectos de redes de electricidad avanzadas).

38 Fifth Domain.

o entidad para distraer la atención o interrumpirlos temporalmente en lugar de causar un daño directo.[39] Un país puede recurrir a este tipo de ciberataque si desea, por ejemplo, neutralizar la ayuda de los aliados de su enemigo durante el tiempo suficiente para lograr un determinado objetivo.[40]

Características particulares e impacto de la guerra cibernética

Aunque la guerra cibernética pueda parecerse a una guerra convencional en algunos aspectos, las características particulares del ciberespacio conllevan nuevas e imprevistas dimensiones. Como los sistemas en el ciberespacio están interconectados mediante ordenadores y redes de comunicación, la interrupción causada por un ataque basado en las TIC no se limita al fallo de un solo sistema, y a menudo trasciende las fronteras nacionales. Los procesos de transferencia de datos pueden afectar a más de un país ya que numerosos servicios Internet se basan en servicios prestados desde el extranjero; por ejemplo, los proveedores de almacenamiento alquilan espacio web a un país cuyos equipos físicos se encuentran en otro. Incluso una breve interrupción de los servicios pueden causar enormes pérdidas financieras a las empresas de comercio electrónico. Las redes de comunicaciones civiles no son los únicos sistemas vulnerables a estos ataques, dado que la dependencia respecto de las TIC también es un importante factor de riesgo para las comunicaciones militares. A diferencia de los soldados tradicionales, los agresores informáticos no necesitan estar presentes cuando se lanza el ataque ni en el lugar desde donde parece provenir. Por otra parte, al lanzar el ataque los agresores pueden utilizar comunicaciones anónimas y tecnología de criptación para ocultar su identidad.[41]

Para efectuar ataques automáticos también se recurre a herramientas informáticas, que pueden encontrarse fácilmente por Internet. Con la ayuda de estos programas informáticos, que llevan ataques preinstalados, un solo delincuente puede atacar miles de sistemas informáticos en un solo día utilizando solamente un computador. Si el delincuente tiene acceso a varios computadores, por ejemplo a través de una red robot, su capacidad de ataque se multiplica. Por ejemplo, el análisis de los ataques contra los sitios web del Gobierno de Estonia indica que se emplearon miles de computadores en una "red robot" o un grupo de computadores infectados que

---

39 *See e.g.*, *Id.* (afirma que "la utilización más probable de las armas cibernéticas no consistirá en crear un apocalipsis electrónico, sino como herramientas para limitar la guerra").

40 *Id.*

41 *CERT Research 2006 Annual Report*, Carnegie Mellon University, Software Engineering Institute, at 7 *et seq.*, www.cert.org/archive/pdf/cert_rsch_annual_rpt_2006.pdf.

ejecutaban programas bajo control externo.[42] Las redes robot hacen aún más difícil rastrear al agresor, por cuanto las pistas iniciales sólo conducen a los demás miembros de la red robot. Según los análisis actuales una cuarta parte de todos los computadores conectados a Internet podrían estar infectados con programas informáticos que los hacen parte de una red robot.

Las herramientas informáticas también simplifican los ataques y permiten que usuarios con menor experiencia en informática y sin conocimientos militares avanzados puedan cometer ciberataques. Huelga decir que los ataques basados en las TIC son, por regla general, más económicos que las operaciones militares tradicionales y pueden proceder de países pequeños. Hoy en día, incluso un país que tradicionalmente tenía muy poca capacidad militar dispone ahora de la posibilidad de inutilizar gravemente la infraestructura esencial de sus enemigos mediante ciberataques. Esta posibilidad de asimetría suscita el interés por la guerra cibernética como estrategia para equilibrar unas condiciones que, de otro modo serían parecidas a las de *David contra Goliat*. El miedo a una guerra cibernética y los ciberataques producidos hasta ahora (aunque limitados), menoscaban la confianza pública en las TIC. Así pues, el efecto dominó psicológico del conflicto cibernético podría tener amplias repercusiones, afectar la utilización eficaz de las nuevas tecnologías e impedir el progreso en muchos sectores.

---

42 *Understanding Cybercrime: A Guide for Developing Countries*, at 72, International Telecommunication Union, April 2009, www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf (en adelante, "Understanding").

3 Dependencia y confianza social

3.1 La dependencia de las sociedades modernas respecto de las TIC e Internet

Por Jacques Bus

Los computadores y las tecnologías de la información nos acompañan desde la segunda mitad del siglo pasado e Internet comenzó a funcionar hace tan sólo 38 años como una red de comunicación en el marco del proyecto ARPA (DARPA). Ahora bien, ha sido en estos últimos 15 años, gracias a la invención de la World Wide Web (por razones prácticas, en el resto de este artículo nos referiremos a "Internet" para designar la combinación de Internet y la web), que Internet se ha extendido a la economía y la vida social a una velocidad trepidante. Hoy en día podemos disfrutar de comunicaciones y redes sociales en cualquier momento y desde cualquier lugar; tenemos acceso a información prácticamente ilimitada; podemos hablar y socializar con personas de todo el mundo; y, además, podemos comparar y comprar servicios y productos tranquilamente desde casa a la hora que queramos.

Según las estimaciones de la UIT para el año 2009, el 25,9% de la población mundial dispone de conexión a Internet (lo que asciende a 1 800 millones de personas). Las personas pasan el doble de horas navegando por Internet que viendo la televisión. Hay unos 4 600 millones de abonados a la telefonía móvil en todo el mundo, lo que representa el 67% de la población mundial. Según Facebook, su número de usuarios activos al mes de julio de 2010 ascendía a 500 millones, mientras que Facebook, Myspace y Twitter recibieron en conjunto unos 220 millones de visitantes activos el mes de julio de 2010. Uno de los cambios más importantes que se han producido en el mundo ha sido la transformación del teléfono móvil en un teléfono Internet, que supera al PC en cuanto a dispositivo preferido para conectarse a Internet. El 9,5% de la población mundial dispone de banda ancha móvil.

Si bien Internet ha alterado la sociedad moderna en ciertos aspectos fundamentales y a escala realmente mundial, aún se esperan muchos cambios más. En muchas publicaciones[43] se describe cómo será el mundo dentro de 25 años. Al parecer, será

---

[43] *Trust in the Information Society: A Report of the Advisory Board RISEPTIS,* www.think-trust.eu/; David-Olivier Jaquet-Chiffelle, ed., *Identity Revolution: Multidisciplinary Perspectives,* FIDIS, mayo de 2009, www.fidis.net/resources/identity-revolution/.

mucho más común utilizar credenciales de identidad para acceder al transporte público, a historiales médicos, a servicios gubernamentales y otros servicios en red. Las redes sociales se expandirán y ofrecerán aplicaciones nuevas, más eficaces y más atractivas. La interrelación de datos dará lugar a la aparición de nuevos servicios de información gracias a los cuales los investigadores podrán a llevar a cabo su investigación de manera más eficaz, los turistas podrán disfrutar mejor de sus viajes, los ciudadanos comprenderán los reglamentos administrativos y los motivos de las decisiones políticas, etcétera. Asimismo, existirán agentes y procesos basados en política que harán por nosotros buena parte de las tareas administrativas, por ejemplo tomar citas, preparar reuniones y cumplir con jurisdicciones.

La revolución social basada en las TIC producirá cambios esenciales en el equilibrio de poder, tanto en el plano nacional, donde los ciudadanos dispondrán de abundante información sobre los procesos políticos que se utilizarán en el proceso democrático, como en el plano internacional. El acceso a Internet aumenta las posibilidades de participación de los ciudadanos en la vida económica y política y les ayuda a comprender la situación y las formas de vida de otras culturas. Hemos visto al Presidente Obama de Estados Unidos utilizar las redes sociales en su campaña y cabe esperar que en el futuro se recurra a actividades similares para obtener el apoyo de la sociedad a las políticas gubernamentales.

Las TIC también permiten que las empresas internacionales se organicen para aprovechar de manera óptima las oportunidades en todo el mundo. Todo esto puede dar un gran impulso al desarrollo económico y al crecimiento globales, en particular en los países donde los costes son pequeños. Algunos grandes países en desarrollo están aprovechando estas oportunidades y se han convertido en importantes actores económicos y políticos.

Ahora bien, como en todas las revoluciones de la historia, junto con las oportunidades y beneficios siempre existe una parte negativa.

Las infraestructuras y los servicios de la información y la comunicación se han convertido en una parte crucial de nuestras economías, pero son extremadamente vulnerables, como ha quedado demostrado por los numerosos ataques que se producen prácticamente a diario. La mayor parte de las otras infraestructuras esenciales, por ejemplo las de energía, agua, transporte y sistemas financieros, dependen sobremanera de las TIC para la comunicación y el control. Así pues, existe un riesgo elevado de accidentes o ataques deliberados contra estas infraestructuras esenciales, que podrían generar el caos y causar enormes pérdidas económicas. Entre estos ataques se cuentan la intrusión y los ataques contra los sistemas y las bases de datos de los organismos nacionales de seguridad.

Esta vulnerabilidad convierte a nuestra infraestructura TIC en objetivo fácil para la "guerra cibernética" o el "ciberterrorismo", lo que supone una amenaza para la estabilidad geopolítica. Se suele denominar "guerra cibernética" a la organización deliberada de ataques contra sistemas esenciales de la sociedad de un país con la aprobación, la ayuda o el control de otro país. Cabe destacar que la palabra "guerra" en este contexto puede prestarse a confusión, dado que en muchos aspectos no es comparable con las connotaciones de esta palabra para muchas personas, a saber, la destrucción prolongada de infraestructura física y la pérdida cuantiosa de vidas.

En los últimos años se han producido varios ataques en los que se utilizó el término "guerra cibernética", por ejemplo en Estonia[44], Georgia, Corea del Sur y Estados Unidos. Estos ataques comienzan a veces con una "guerra" psicológica que llevan a cabo aficionados con fines propagandísticos, y luego comienza una segunda fase en la que participan expertos en ciberataques (delincuentes o no) que consiste en una campaña a gran escala a través de redes robot que lanzan ataques de denegación de servicio contra la infraestructura socioeconómica. En otros casos, los ciberataques se lanzaron justo antes o durante las acciones militares convencionales. Hasta ahora la destrucción causada por los ciberataques era limitada en la mayoría de los casos y la capacidad podía restablecerse después de unos cuantos días, sin que se llegara a perder vidas como consecuencia directa de dichos ciberataques.

El papel que han desempeñado los Estados en estos conflictos ha quedado en general sin demostrar. De ahí la urgencia de concertar acuerdos internacionales sobre las restricciones y la defensa contra ciberataques y para la cooperación internacional con el fin de tenerlos bajo control. Es evidente que el principio de disuasión que imperaba durante la Guerra Fría no es fácilmente aplicable en el ciberespacio. No se entiende bien en qué consistiría tal disuasión y, lo que es aún más importante, es muy difícil de identificar al enemigo (por falta de atribución y porque se recurre a intermediarios).

Dejando de lado el debate político sobre el término "guerra cibernética", no cabe duda de que la ciberdelincuencia se está convirtiendo en un problema muy preocupante. El número de amenazas debidas a código maléfico y delictivo aumenta exponencialmente. En sólo 2008, Symantec detectó 1,6 millones de amenazas, lo que representa el 60% del total de las amenazas detectadas en todos los años anteriores a 2008. Más de 8 millones de residentes en Estados Unidos fueron víctimas de un robo de identidad. El costo en promedio del robo de datos en los Estados Unidos se ha

---

[44] Véase también Kertu Ruus, "Cyber War I: Estonia attacked from Russia," *European Affairs*, Vol.9, No1-2, 2008, http://findarticles.com/p/articles/mi_7054/is_1-2_9/ai_n28550773/.

estimado en unos 6,7 millones USD. En febrero de 2010 se publicó que los sistemas informáticos de unas 750 000 empresas de todo mundo estaban infectados y controlados por redes robot. El Sr. Amit Yoran, antiguo representante de Estados Unidos, sugirió que las empresas no están preparadas para defenderse, aunque la industria de seguridad de Estados Unidos le restara luego importancia a esta afirmación.

El Sr. Howard Smith (Asistente Especial del Presidente de Estados Unidos y Coordinador de Ciberseguridad) reconoció que la utilización malévola de Internet es un problema cada vez mayor, aunque indicó prioridades claras. Rechazó el término "guerra cibernética" por considerarlo un "concepto atroz". A su juicio, no hay vencedores en ese entorno y propone que nos deberíamos concentrar en la delincuencia y el espionaje en línea.

A pesar de las diferentes opiniones, hay un consenso general de que existen motivos para alarmarse en lo que respecta a la seguridad y la confianza en Internet. Los riesgos actuales tienden a aumentar el miedo y el rechazo de los ciudadanos al nuevo universo digital. Si los políticos y la tecnología no fueran capaces de resolver estos aspectos negativos de la sociedad, las consecuencias económicas serían enormes.

En su discurso del 21 enero 2010, Hillary Clinton, Secretaria de Estado de Estados Unidos, destacó la importancia de que Internet sea abierta y libre para la cooperación y el desarrollo a escala mundial. Hizo referencia a las "cuatro libertades" de Roosevelt (libertad de expresión y de culto y libertad para vivir sin miseria y eludir el miedo) y al importante efecto de Internet sobre estas libertades, especialmente la libertad de expresión. Internet ha desencadenado una revolución en el intercambio de información y las redes sociales. Además, tiene un enorme potencial para crear más riqueza para todos, en particular cuando se reconoce plenamente la "libertad de conexión". Sin embargo, también ha dado lugar a un aumento de delincuencia mundial y a la aparición de miedo, que es necesario contener.

Los políticos han reconocido claramente la enorme importancia de Internet en el plano geopolítico mundial. Saben que los ciudadanos esperan que el gobierno les ofrezca seguridad y protección, pero la jurisdicción nacional y las fronteras ya no consiguen ofrecer esta seguridad y protección del mismo modo que antes. La legislación en materia de protección del consumidor tal como se aplica en muchos países, así como la responsabilidad por el producto o servicio, ha perdido su vigencia en un mundo donde el cliente y el proveedor se encuentran en jurisdicciones diferentes que no cooperan entre sí y donde los servicios se prestan a través de unas cadenas especializadas de subservicios que emplean datos procedentes de nubes distribuidas por todo el planeta.

Los líderes mundiales tienen que hacer frente a unos desafíos enormes y sin precedentes. El cambio climático y los rápidos cambios en el poder económico mundial y en la seguridad energética, por citar algunos, requiere la atención política, como también los riesgos que entraña la conexión digital a escala mundial. Para solucionar todos estos problemas tendremos que asumir un liderazgo firme y visionario a escala mundial.

Lo más importante de todo es aprovechar lo que hemos aprendido a lo largo de la historia acerca de las estructuras y los valores sociales, la seguridad, la confianza y las relaciones internacionales. Tenemos que iniciar una transformación mundial para transponer nuestros valores culturales y sociales y nuestra fortaleza, y comenzar un proceso de cooperación internacional que resulte útil en un mundo que reconoce la realidad de la interconexión digital.

Necesidad de confianza

El concepto de confianza y su función en la sociedad

"*La confianza domina la vida cotidiana. Si tomamos sólo una pequeña muestra del apabullante número de ocasiones en las que entra en juego la confianza, podemos observar que de todos los fenómenos sociales la confianza es, sin duda, uno de los más importantes. El hecho de que sea tan esencial dificulta su estudio. ¿Cómo podemos llegar a comprender una fuerza social tan proteica?*"[45]

La confianza y la fiabilidad son conceptos básicos de la existencia humana. Los utilizamos de manera intuitiva y su significado depende siempre del contexto. Ahora bien, al transponer estos conceptos al entorno digital nos encontramos fácilmente con problemas.

Luhmann[46] explica que la confianza es un mecanismo que reduce la complejidad y permite a las personas sobrellevar los elevados niveles de incertidumbre y complejidad de la vida (contemporánea). Así pues, la confianza aumenta la capacidad de las personas de relacionarse satisfactoriamente con el mundo real, cuya complejidad e incertidumbre es mayor de lo que somos capaces de aceptar. En este sentido, se necesita un mecanismo que permita a las personas seguir viviendo:

---

[45] Kieron *O'Hara, Trust: From Socrates to Spin*, Icon Books, Cambridge, 2004, pág. 10, http://eprints.ecs.soton.ac.uk/9361/.

[46] Niklas Luhmann, *"Trust: A Mechanism for the Reduction of Social Complexity", Trust and Power*, New York: Wiley, 1979 at 4-103.

comunicar, cooperar, realizar transacciones económicas, etcétera. Este concepto enriquece la vida de cada persona, dado que fomenta la actividad, la audacia, la osadía y la creatividad, y enriquece las relaciones individuales con los demás.

Visto desde otra perspectiva, podemos afirmar que la confianza es la expectativa de que la parte en la que se confía se comportará de manera benévola en una determinada situación. Como bien explica Hardin[47]: "la confianza se encuentra en la misma categoría cognitiva que el conocimiento y la creencia. Decir que confío en ti es lo mismo que decir que sé o creo saber ciertas cosas sobre ti que me hacen suponer que eres digno de mi confianza y que actuarás de manera "benévola" en circunstancias impredecibles".

La confianza es una relación tripartita (*A* confía en que *B* hará *X*). La evaluación de la confianza que *A* tiene de que *B* hará *X* desempeña un papel importante cuando *A* tiene que decidir si participar o no en cualquier transacción, intercambio o comunicación con *B*. Al reducir la complejidad y el riesgo percibido, la confianza facilita efectivamente la actividad económica, la creatividad y la innovación. Huelga decir que la confianza depende sobremanera del contexto y que es contingente en lo que respecta a variables como: el tiempo (uno puede perder fácilmente la confianza en alguien, pero el concepto propiamente dicho también cambia con el paso del tiempo); la historia y la memoria; el lugar y la situación; la cultura; el tipo de relación (privada o profesional); los sentimientos; y otras variables (por ejemplo, las consideraciones sociológicas tales como la reputación, la repetición y la recomendación).

De lo anterior se desprende que la confianza es un concepto que puede ir aumentando en una determinada situación y entre dos partes dadas. El hecho de disponer de más información, ya sea por medio de otros indicadores o de relaciones, puede contribuir a reforzar la confianza y a prolongar la duración de una relación satisfactoria.

Por lo general, en el análisis que figura a continuación consideraremos que las partes *A* y *B* son seres humanos. Ello no excluye la posibilidad de que estas personas actúen en nombre de organizaciones o grupos. En la práctica, muchas personas utilizan también el término confianza al referirse a la relación con otras entidades, por ejemplo con el gobierno, una empresa, un sistema o servicio, una base de datos o un servicio de información (por ejemplo un periódico, una bitácora sobre tecnología) e incluso a una entidad virtual como un agente informático. Hardin denominaría a esto como "confianza en la forma de actuar, el comportamiento o la integridad de la entidad".

---

47 Russell Hardin, *Trust and Trustworthiness*; Russell Sage Foundation Series on Trust, Vol. 4, 2002.

Esta confianza podría crearse, por ejemplo, mediante rendición de cuentas, transparencia, garantías y responsabilidades, auditorías, o por el mero hecho de conocer la reputación o las intenciones de la entidad.

El concepto de confianza en cuanto capital social o "fideicomiso social" ha sido analizado y elaborado por Fukuyama[48], Putnam[49] y otros expertos. Se trata de un concepto estadístico que representa la opinión de los ciudadanos sobre el grado de confianza que merece su sociedad en todos sus aspectos, o, para ser más precisos: la confianza que tienen los ciudadanos en el gobierno, las instituciones, el ordenamiento jurídico, los sistemas, etc. de la sociedad. Al parecer, existe una fuerte correlación entre el grado de confianza social y el crecimiento y la prosperidad económica, de modo que cuanto mayor sea lo primero mayor será también lo segundo.

Nosotros utilizaremos el término "confianza" en el sentido que Hardin le da al término "fiabilidad". Ahora bien, en adelante conviene tener presente que es importante distinguir la confianza entre las personas que utilizan sistemas y servicios digitales en sus interacciones, y la confianza o fiabilidad de una persona en una entidad o institución no humana.

La introducción de la tecnología digital ha revolucionado la comunicación y la cooperación humanas gracias a la introducción de un nuevo intermediario, que consiste en un conjunto complejo de "instituciones" tecnológicas (las redes, los servicios digitales, las bases de datos, las redes sociales, etc.). Así, al analizar la confianza entre seres humanos debemos tomar en consideración el aspecto de la confianza (o fiabilidad) en esta infraestructura tecnológica.

Nissenbaum[50] examina solamente la confianza entre personas que utilizan sistemas digitales en red para su comunicación y enumera una lista de factores que afectan sistemáticamente a la tendencia a confiar (o a no confiar):

1. Historia y reputación
2. Deducciones basadas en las características personales: por ejemplo la virtud, la prudencia, la lealtad, el deseo de que los demás tengan una buena opinión, el comportamiento, la forma de vestir.

---

48 Francis Fukuyama, *Trust: The Social Virtues and the Creation of Prosperity*, Free Press, 1995

49 Robert D. Putnam, Robert Leonardi, and Raffaella Y. Nanetti, *Making Democracy Work: Civic Traditions in Modern Italy,* Princeton University Press, 1993

50 Helen Nissenbaum, "Securing Trust Online: Wisdom or Oxymoron?" Boston University Law Review, Vol. 81, No. 3, June 2001 at 635-664, www.nyu.edu/projects/nissenbaum/main_cv.html .

3. Relaciones: mutualidad y reciprocidad, ser familia, estar en el mismo barco, tener objetivos comunes.
4. La función que desempeñan (piloto, conductor de bus).
5. Factores contextuales (grupos y comunidades, publicidad; recompensas y sanciones; normas; garantías y seguridad, como la responsabilidad jurídica o la legislación en materia del consumidor).

Varios de estos factores, en particular el 1 y el 3, guardan relación con la "confianza en cuanto interés inherentes" tal como la define Hardin.[48] A la persona en que se confía le interesa actuar correctamente para, por ejemplo, no perder su reputación ya que ello podría quebrar la relación con la persona que en él confía (por ejemplo, un piloto que pierde su reputación puede perder su empleo). Hardin también enumera los obstáculos a la confianza de línea:

1. no existen identidades (pero observa el derecho al anonimato);
2. no existen características personales (pero observa el derecho a la privacidad);
3. contextos inescrutables (desconocidos y confusos, lo que crea cierta obscuridad, aunque también ofrece libertad).

El tercer punto podría considerarse simplemente como que existe mayor complejidad en línea. Desde luego ofrece más libertad pero, al mismo tiempo, para llevar a cabo una transacción o una comunicación de manera adecuada será necesario crear aún más confianza y, por ende, dependencia. Nissenbaum también indica que la seguridad no crea confianza. Si existe seguridad, no hay necesidad de confianza. Ahora bien, la confianza permite a las personas vivir en un mundo muy inseguro y complejo; al aumentar la seguridad se reduce su riqueza y complejidad. Otros autores consideran que la seguridad se encuentra en un extremo de la escala de confianza mientras que en el otro extremo estaría la confianza totalmente infundada (ingenuidad).

El hecho de que la confianza en la infraestructura mundial de la información (en el extranjero) esté aumentando a medida que se conoce mejor ha llevado a que la revista *The Economist* afirme lo siguiente: "El hecho de que tantas personas deseen tener la oportunidad […] de vivir en otros países distintos del suyo, deja sin sentido el consenso arraigado en política y filosofía de que el animal humano donde mejor está es en su casa".[51] Añade además que: "El error de la filosofía ha sido suponer que el

---

51 "The Others," *The Economist*, 17 de diciembre de 2009, www.economist.com/node/15108690.

hombre, por ser un animal social, debe pertenecer a una determinada sociedad".[52] No obstante, esto podría considerarse como una generalización del comportamiento de una minoría, ya que siguen siendo una escasa minoría los que no recurren a vacaciones totalmente seguras y organizadas por una agencia de viajes desde su país.

Sin embargo, la globalización, que se ha visto impulsada claramente por las TIC y la web, fomenta la comprensión y, por ende, infunde mayor confianza gracias a la divulgación de información sobre la historia, la reputación y las características de las sociedades, así como el estilo de vida de los habitantes de determinadas sociedades. Además, facilita la comunicación a escala mundial. Todo esto puede erosionar aún más la idea de que "el animal humano donde mejor está es en su casa". Incluso podría ser necesario adoptar una perspectiva completamente nueva sobre las sociedades y su cohesión, así como la función que debe desempeñar la confianza en las mismas.

Confianza en la sociedad digital

Como hemos mencionado antes, debemos distinguir entre:

- La confianza entre personas de una sociedad que utilizan considerablemente la tecnología digital para la comunicación y las transacciones.
- La confianza o fiabilidad que tienen las personas en la infraestructura de las redes y sistemas digitales que utilizan para servicios, comunicaciones, almacenamiento de datos, cálculo, etc.

Comencemos por el primer punto.

Los problemas de la confianza (entre personas) en la sociedad digital, en comparación con la "sociedad antigua", guardan relación especialmente con:[53]

- La transformación que se ha producido en la manera de recabar, almacenar, procesar, poner a disposición y proteger datos. No sólo se recaban y almacenan datos producidos por personas con objeto de comunicación y almacenamiento, sino que también se recaban datos sobre los hábitos de conducta mediante la vigilancia (por ejemplo, se observa a las personas cuando pasean por la calle, consultan una página web o abren un anuncio en la web).
- Los conceptos de identificación, reputación, autentificación y responsabilidad tienen un significado diferente en Internet. Para convencer a otra persona de

---

52 *Id.*

53 *Véase* Nissenbaum.

la identidad de uno, se necesita demostrar atributos o proporcionar secretos o información biomédica. La reputación puede verse fácilmente arruinada si se divulga información ofensiva o falsa, que resulta luego extremadamente difícil de corregir. La posibilidad de ocultarse en otras jurisdicciones menoscaba considerablemente los principios de responsabilidad y transparencia cuando no hay acuerdos internacionales de arresto y extradición.

- El aumento de la complejidad, la tecnología incomprensible sin garantías suficientes de certificación y normalización, y la falta de transparencia de los procesos y métodos de recopilación y utilización de datos, han creado un contexto inescrutable que merma la confianza que debe haber entre las personas en el entorno digital. Las personas pueden quedar perplejas con lo que sucede a su alrededor y a menudo no tienen idea de qué datos personales se están recabando y cómo se utilizan.

Es más fácil crear confianza cuando se conoce la identidad y/u otra información de autentificación (credenciales, atributos o alegaciones) de la otra parte o dicha identidad puede confirmarse (posiblemente por medio de un tercero fiable). La reputación u otra información procedente de la web o de amigos en una red social pueden contribuir a la confianza. Por otra parte, los ciudadanos tendrían más confianza en una transacción con un tercero si pudieran controlar el grado de exposición e intercambio de sus datos con dicha parte. Esta confianza también aumentará con la transparencia de las operaciones de recopilación y procesamiento de datos y con la buena reputación de tales entidades.

Ahora bien (y con esto pasamos al segundo punto), en nuestro universo tecnológico la confianza entre personas sólo puede obtenerse si podemos fiarnos de los sistemas utilizados para comunicar, intercambiar datos o confirmar la identidad u otra información, por ejemplo la reputación o las credenciales. Para utilizar Internet, los ciudadanos deben tener confianza en las herramientas, sistemas e infraestructuras que utilizan para sus transacciones y comunicaciones. Decimos que un sistema o servicio es *fiable* hasta un cierto nivel, si la persona puede tener un determinado grado de confianza justificable en que el sistema o servicio funcionará de acuerdo con su descripción y promesas, y que no efectuará acciones que no están descritas en diversas circunstancias. La confianza justificable puede obtenerse mediante la responsabilidad (responsabilidad por el producto), la transparencia en el procesamiento y almacenamiento de datos, la certificación de sistemas técnicos y la capacidad de verificación *a posteriori*. También puede verse reforzada por el suministro de herramientas y mecanismos comprensibles y útiles que permitan confirmar las credenciales, la reputación o la identidad alegadas. Las personas

necesitan servicios y herramientas que los ayuden a crear y reforzar la confianza en la calidad del servicio, la seguridad, la robustez, la protección de los datos y la privacidad, con arreglo a políticas predefinidas y comprensibles. Estas herramientas podrían proporcionarlas los proveedores de servicio que actúen como terceros y las autoridades públicas.

Como explica Vitali Tsygichko[54], los sistemas de información automáticos (AIS) desempeñan una función importante en la sociedad moderna y cada vez están más integrados en los sistemas de la administración pública de todos los sectores del país. Estos sistemas AIS constituyen el núcleo de los sistemas de gestión de decisiones en prácticamente todas las organizaciones socioeconómicas. Lo que está en juego no es exclusivamente de la eficiencia de las autoridades públicas, de las instituciones económicas y de las organizaciones voluntarias, sino también la seguridad nacional, que depende sobremanera del correcto funcionamiento de estos sistemas.

No cabe duda de lo extremadamente importante que resulta examinar la fiabilidad de estos sistemas. Ésta guarda relación sobre todo con la validación de los modelos subyacentes, la fiabilidad de la infraestructura lógica y física, el nivel de cualificación profesional del personal encargado del mantenimiento del sistema y la eficacia de las medidas de protección contra amenazas externas.

Según argumenta Tsygichko, la fiabilidad de los AIS requiere la elaboración de un conjunto de requisitos y métricas en materia de seguridad, fiabilidad (incluido el modelo subyacente de representación de la realidad) e integridad de los datos. Podría utilizarse como criterio un parámetro que cuantifique el riesgo a burlar la seguridad. La **gestión de riesgos** se define como los procesos para determinar y analizar los riesgos y tomar decisiones, que comprende el hacer máximas las repercusiones positivas y mínimas las consecuencias negativas ante cualquier eventualidad.

Además de los medios técnicos necesarios para instaurar confianza, necesitamos normas, reglamentos y cierta aceptación social. Los ciudadanos confiarán en la gestión de sus datos personales dentro de su sociedad si: se respeta y aplica la reglamentación en materia de protección de datos personales y privacidad; las organizaciones cumplen con las expectativas de los ciudadanos en cuanto a una cultura de responsabilidad que conste de una reglamentación adecuada para la protección y compensación del consumidor; existe una reglamentación sobre verificación y transparencia; y las responsabilidades en la cadena de actores que participan en una transacción están claramente asignadas.

---

54 Vitali Tsygichko es un miembro asociado del PMP InfoSecur y participó en estas deliberaciones.

A nivel de política general, la fiabilidad de la infraestructura TIC sólo puede lograrse y mantenerse con incentivos adecuados y debidamente distribuidos a lo largo de toda la cadena de valores.

La transparencia y la responsabilidad son necesarias para garantizar la justicia y la aplicación de la ley. Es necesario resolver los problemas relacionados con la responsabilidad por los sistemas y, en particular, por las partes relacionadas con los programas informáticos y la integridad de los datos. Podría crearse un sistema de seguros de riesgo contra violación de la seguridad, que a su vez fomentaría el desarrollo de medidas y herramientas para evaluar los riesgos. Todo esto podría culminar en un sistema en gran medida autorregulado y sostenible.

Un requisito esencial para infundir confianza a las personas que utilizan Internet es el desarrollo de un sistema fiable y compatible a escala mundial para la **identificación y autentificación**. El desarrollo de tarjetas de identidad y pasaportes electrónicos fiables por parte de los gobiernos, con arreglo a normas convenidas en el plano internacional, es un ejemplo que han seguido muchos países. Sin embargo, para las transacciones electrónicas mundiales necesitamos un sistema compatible de gestión de credenciales y de reclamaciones por Internet que garantice el cumplimiento de los derechos de privacidad. La responsabilidad es esencial para la economía de Internet y sólo puede lograrse si existe una verdadera responsabilidad jurídica de las personas y organizaciones por sus actividades contractuales y públicas. Para esto último se recurre normalmente a credenciales, que demuestran los atributos o utilizan secretos que sólo conoce la persona del caso. Dependiendo de la situación pueden emplearse diferentes tipos de secretos, credenciales o atributos, lo que da lugar a diferentes "identidades". Cameron, Posh y Rannenberg han propuesto normas a nivel de metadatos para la gestión de identidades alegadas.[55]

Internet consta de muy diversas redes sociales que ofrecen la oportunidad a las personas y las organizaciones de crear sus diarios, círculos de amistades y reputaciones en diversas comunidades. En la terminología del proyecto FIDIS[56] esto conduciría a "identidades parciales" de una persona. En situaciones que exigen responsabilidad, estas identidades pueden relacionarse, mediante un mecanismo de

---

[55] Kim Cameron, Reinard Posch, and Kai Rannenberg, *Proposal for a Common Identity Framework: A User-Centric Identity Metasystem,* Joint 'ICT Security' – 'ICT for Government and Public Services' Workshop on "Identity Management in the Future Digital Society, 14 Oct. 2008, www.identityblog.com/?p=1048.

[56] "About the FIDIS Network of Excellence," www.fidis.net/about/.

protección de la privacidad, para la identificación, autentificación y firmas digitales. También podrían contribuir a proporcionar mayor confianza en Internet en tanto que mecanismo para actividades socioeconómicas.

Resumen

Hemos examinado la importancia que reviste la confianza en nuestra sociedad desde distintos puntos de vista. En particular, hemos explicado los cambios y problemas que están surgiendo a medida que nuestra sociedad se hace cada vez más dependiente de las comunicaciones y transacciones digitales por Internet. La carencia de un mecanismo de identificación adecuado que respete el derecho al anonimato en algunos casos, la imposibilidad de percibir las características personales junto con la necesidad de proteger la privacidad y, por último, pero no por ello menos importante, el contexto inescrutable creado por la infraestructura de tecnología utilizada en nuestras comunicaciones, ha desprovisto a los seres humanos de los mecanismos esenciales para tener confianza y que les permita vivir y ser creativos en la sociedad mundializada.

Por consiguiente, debemos crear nuevos mecanismos de confianza en el universo digital que permitan a las personas confiar unas en otras, con independencia del lugar donde se encuentren y la forma en que se conozcan.

Debemos velar por disponer de redes de comunicaciones seguras y fiables; sistemas informáticos que ofrezcan garantías sobre el cumplimiento de la legislación en materia de privacidad y protección de datos; un marco mundial y compatible fiable para la identificación y gestión de credenciales/alegaciones; y servicios que asuman su debida responsabilidad y cumplan la legislación en materia de protección del consumidor. Esta tecnología debe concebirse y desarrollarse teniendo presente la confianza, la seguridad y la privacidad, y debe permitir la aplicación de la ley y la transparencia. Asimismo, la legislación y la reglamentación debe elaborarse teniendo presente las tendencias y el potencial de la tecnología.

Es preciso que los sectores público y privado colaboren en el plano internacional con el fin de crear una infraestructura equilibrada de tecnología y legislación/reglamentación que infunda a los ciudadanos la confianza necesaria para aprovechar las oportunidades que ofrece el nuevo universo digital.

De esta forma, la humanidad conseguirá generar oportunidades sin precedentes hasta ahora para comunicar, cooperar y efectuar transacciones económicas a escala mundial basadas en mecanismos fiables, tan fiables como la interacción directa entre humanos en las comunidades pequeñas que existían en el pasado. Esto constituirá un gran paso hacia la estabilidad mundial.

3.2 Repercusiones socioeconómicas de la ciberdelincuencia

Por Jacques Bus[57]

La prestación de servicios digitales, y en general la infraestructura digital que se está desarrollando en nuestra sociedad, tiene un enorme potencial positivo. Ahora bien, como sucede con cualquier tecnología, ésta puede utilizarse para fines malévolos. Podemos distinguir los siguientes cuatro aspectos problemáticos en relación con las cuestiones socioeconómicas:

1) **El carácter global del espacio digital:** La aparición de servicios transfronterizos y la comunicación por Internet ha creado una serie de problemas de confianza social y económicos, así como problemas de seguridad nacional que hasta ahora se resolvían dentro del territorio del país (control de importaciones y exportaciones, control de pasaportes, aduanas, agresión entre países, etc.) o dentro del Estado mediante operaciones policiales a escala local o nacional contra los ciudadanos fichados. Las consecuencias negativas de la ausencia de controles fronterizos en el espacio digital apenas se han abordado de manera sustantiva, ni en el plano nacional ni en el internacional. Es evidente que esta falta de control facilita la delincuencia puesto que ofrece cierta inmunidad a los delincuentes, en parte porque las acciones que se cometen por la web son muy difíciles de atribuir a quien las ha cometido, y en parte porque estos delincuentes se encuentran en países que les ofrece protección contra la aplicación de la ley internacional.

2) **Complejidad de los servicios:** Las transacciones y servicios por la web consisten cada vez más en cadenas especializadas de subservicios distribuidos en diversas jurisdicciones y que utilizan datos procedentes de todas partes de la nube. Los subservicios o los datos pueden ofrecerse desde distintos regímenes jurisdiccionales, incluso contradictorios. A los consumidores les resulta difícil reparar en este hecho y comprender las consecuencias. Los Estados ya no pueden garantizar la responsabilidad jurídica por el producto ni la protección de los consumidores de la forma en que lo hacían hasta ahora. Para ello necesitarían acuerdos y cooperación internacionales para aplicar la ley. Asimismo, los servicios tienen que garantizar la trasparencia en la cadena de servicios y responder (automáticamente) a las condiciones que establezcan los consumidores. La situación actual, junto con lo mencionado en el punto 1, ofrece enormes posibilidades para realizar estafas y

---

[57] El autor desea agradecer la contribución de Udo Helmbrecht y su equipo en la ENISA (Agencia Europea de Seguridad de las Redes y de la Información).

fraudes sin dejar rastro. Hoy en día los Estados no pueden ofrecer protección contra esto.

3) **Redes sociales y salas de charla:** A menudo se utilizan para hacer contactos con fines malévolos, y están especialmente destinados a niños y ancianos. Esto no es nada nuevo. Los fraudes y estafas siempre han existido. Ahora bien, la deficiente autentificación y la falta de seguridad y de mecanismos de protección de la privacidad para credenciales (como el nombre, la fecha de nacimiento, la edad, el sexo, los datos sobre el empleo, las contraseñas) hacen que sea muy fácil y lucrativo recurrir a estos artificios. Los virus también han llegado a los sitios de redes sociales, en los que la confianza puede utilizarse como vector. La tasa de éxito de los ataques que utilizan redes sociales es muy alta. La mayor amenaza en relación con los bancos es la *peska* (phishing), pero los bancos todavía no ofrecen servicios de autentificación para sus clientes.

4) **Organización internacional de la delincuencia:** En los últimos años se ha informado de que la delincuencia internacional está recurriendo a la web para conseguir sus objetivos delictivos, pero que además existe un mercado negro internacional que colabora para crear herramientas criminales (redes robot, herramientas de *peska*, virus, etc.) y robar datos (información personal, datos de tarjetas de crédito, información confidencial de empresas). La delincuencia que utiliza y se comete por la web está cada vez mejor organizada en el plano internacional, abarca muchas jurisdicciones, sobre todo en las que el poder judicial es muy débil, y se concentra principalmente en fines lucrativos. Existen muchos ejemplos de esta evolución. La FTC cerró una empresa de software maléfico semilegal el mes de marzo con una cifra de negocios de más de 180 millones USD. Existen garantías de devolución del dinero sobre virus, asistencia técnica y ciberutensilios de "bricolaje" para cometer actos delictivos. El troyano para bancos Zeus cuesta 700 USD (4000 USD la última versión) en el mercado negro (Zeus se utiliza para burlar los sistemas de autentificación tales como los basados en dos factores y el sistema de código de seguridad de la tarjeta MasterCard). Existen varios estratos de proveedores legales y semilegales que sacan beneficios de la economía sumergida.

Los estudios y estadísticas dan a veces cifras asombrosas de las pérdidas económicas y sociales que causan estas actividades ilícitas. Estas cifras pueden alcanzar 1 billón

USD[58] en todo el mundo, lo que representa alrededor del 2% del PIB mundial. Boston Computing Network estima que las empresas americanas perdieron más de 7 600 millones de dólares debido a los virus durante los primeros seis meses de 1999. En Alemania, las cifras de pérdidas financieras a causa de la *peska* se estiman en 15 millones de euros al año, mientras que las relacionadas con las tarjetas de crédito ascienden a 155 millones de euros.

En general, la mayoría de las cifras sobre pérdidas económicas se basan en hipótesis discutibles y extrapolaciones necesarias a partir de los datos que se conocen, aunque muchos problemas no se hacen públicos. No obstante, puede llegarse la conclusión de que el coste socioeconómico de la ciberdelincuencia es muy importante y a menudo subestimado por quienes toman las decisiones en materia de inversión en medidas de seguridad. La recuperación de las inversiones en seguridad debe examinarse mucho más detenidamente.

La lucha contra la ciberdelincuencia exige que se asignen responsabilidades jurídicas por las acciones cometidas en el entorno digital. También deben quedar comprendidas las pequeñas contribuciones a servicios internacionales creados dinámicamente. La cooperación jurídica y diplomacia de las altas instancias en el plano internacional son indispensables a la hora de definir políticas y procedimientos comunes que creen fiabilidad y responsabilidad en relación con los servicios y las actividades económicas y públicas.

Se necesitan soluciones técnicas que, por una parte, permitan preservar la cohesión de la red mundial, para que las empresas y los consumidores tengan acceso a la misma para trabajar, comunicarse y obtener información desde sus hogares o cuando estén de viaje, de manera que se garantice el cumplimiento de la legislación aplicable a todas las instancias de la actividad, mientras que, por otra parte, respeten el derecho a la vida privada en la web y, por ende, las personas tengan la posibilidad de navegar por la web dentro de los círculos de confianza seguros y reducidos que ellos elijan en determinadas situaciones y con las garantías por parte de los proveedores de que el intercambio de datos no se utilizará para otros fines.

---

58 "McAfee, Inc. Research Shows Global Recession Increasing Risks to Intellectual Property," McAfee Press Release. Febrero de 2010, www.mcafee.com/us/about/press/corporate/2009/20090129_063500_j.html; véase también Unsecured Economies Protecting Vital Information, McAfee, 2009, http://resources.mcafee.com/content/NAUnsecuredEconomiesReport

Lamentablemente, estamos siendo testigos de la aparición de una economía de datos privados que va en la dirección opuesta. Las empresas de recopilación y procesamiento de datos obtienen sus beneficios exclusivamente a partir de un modelo comercial que gira en torno a los datos de sus clientes privados. Los consumidores pueden pensar que son clientes de estos proveedores de servicios y que, por lo tanto, estos proveedores son responsables del servicio. Pero en realidad, el consumidor no paga nada a estas empresas, puesto que en realidad ellos son el producto. Las empresas de comercialización, de análisis de datos, de creación de perfiles, de publicidad y otras empresas son los VERDADEROS clientes, a quienes los sitios de redes sociales, los portales de servicios, etc. les venden los datos de los consumidores.

En realidad, la vida privada parece haberse convertido en la víctima real del progreso en el espacio socioeconómico creado por el mundo digital y la conexión en red. El precio del almacenamiento de datos disminuye muy rápidamente y al final los datos podrán almacenarse sin límite de volumen ni de tiempo. Esto afectará profundamente a la forma en que interactuamos y creará nuevos delitos en el futuro (ruptura de la privacidad, creación de perfiles no autorizados, minería de datos no autorizada), así como nuevas formas de control político. Muchas de estas actividades podrían atentar contra los derechos constitucionales vigentes y apenas se han examinado las repercusiones que ello tendría para la estabilidad social, económica y política de la sociedad.

Además de los posibles efectos del entorno digital sobre la delincuencia y los derechos humanos antes mencionados, existe otro peligro totalmente diferente para la sociedad y las economías que guarda relación con la formidable vulnerabilidad de la futura infraestructura social digital. Puede suceder que las sociedades en su conjunto tengan que hacer frente a pérdidas económicas y sociales cuando se produzcan ataques contra sus redes de comunicaciones y otras infraestructuras esenciales y éstas queden interrumpidas, ya sea por delincuentes (con fines de extorsión), por terroristas para infundir miedo e inestabilidad, o por otros Estados en el marco de una guerra o conflicto. La capacidad de los Estados para reaccionar contra tales ataques se reduce prácticamente a medidas defensivas. Muchas estrategias ofensivas, como la disuasión o el contraataque, son difíciles de efectuar, por cuanto a menudo los ataques no son atribuibles y comienzan en lugares desconocidos o Estados parias. Si no se confiere suficiente atención a la seguridad y la confianza en las redes y sistemas, el desarrollo tecnológico no hará sino agravar estos problemas y puede dar lugar a que los conflictos nacionales e internacionales sean incontrolables en el futuro.

Por último, otro aspecto esencial que debe considerarse es el riesgo a largo plazo para la sociedad. Los ataques pueden durar sólo unos segundos y tener efectos de consideración. Puede tardarse años en recuperar la confianza social perdida en esos

segundos. El menoscabo de la confianza entre personas, entre las personas y empresas, entre los ciudadanos y su Estado, y entre Estados puede tener efectos devastadores en las sociedades y en la estabilidad mundial a largo plazo. Asimismo, puede constituir un obstáculo para el futuro crecimiento económico, que depende sobremanera en un aumento en la utilización de las TIC tras la última crisis económica. No podemos permitirnos el lujo de quedar estancados debido a la pérdida de confianza.

La seguridad de la información y de las redes, incluida la autentificación, en el entorno digital debe garantizar la seguridad de los ciudadanos (física, económica y privada). Los sistemas, infraestructuras e instituciones de TIC fiables garantizarán un nivel de confianza pública en nuestras sociedades que resulta fundamental para la prosperidad económica, como se indica en numerosos estudios.

La inestabilidad social y los daños económicos (en lo que respecta al crecimiento económico) son difíciles de cuantificar, pero pueden llegar a ser considerables. Por consiguiente, es necesario estar preparados y muy protegidos, así como disponer de sistemas que se recuperen rápidamente y se reparen solos.

En resumen, podemos afirmar:

El carácter mundial del espacio digital, caracterizado por una identificación deficiente de los usuarios y una atribución insuficiente de acciones, la complejidad de los servicios distribuidos a escala internacional, el desarrollo mundial de sitios de redes sociales, y la aparición de redes y mercados internacionales de delincuencia resultan muy preocupantes en lo que respecta al aumento de la ciberdelincuencia y, por consiguiente, la sostenibilidad de una sociedad estable, que es el pilar sobre el que reposa el desarrollo personal y la prosperidad económica.

La vulnerabilidad de nuestras infraestructuras de TIC sociales y la recopilación y almacenamiento ilimitado de datos atentan contra la libertad personal y la estabilidad internacional.

La confianza que los ciudadanos tienen en la sociedad y el gobierno para mantener la paz, la seguridad y la prosperidad puede verse erosionada por los peligros y la incertidumbre generados por los adelantos tecnológicos, con posiblemente grandes pérdidas económicas.

Por consiguiente, necesitamos urgentemente la adopción de medidas políticas de alcance mundial para resolver estos problemas, basadas en un análisis sólido de las tendencias tecnológicas, sociales, económicas y políticas y sus consecuencias.

4 Tendencias y amenazas tecnológicas

4.1 Potencial actual, tendencias y amenazas

Por Axel Lehmann, Vladimir Britkov, Jacques Bus

Las fuerzas que dan lugar a innovaciones en los productos son "impulsos" tecnológicos o "tirones" del mercado. A este respecto, los análisis de las futuras direcciones y posibilidades de las innovaciones en las TIC deben considerar los avances tecnológicos actuales y previstos, así como las tendencias en las futuras demandas de los consumidores y del mercado. Por tanto, las tres primeras secciones de este capítulo abordan a esas tendencias y demandas, presentan un análisis de las principales amenazas y hacen algunas observaciones a modo de conclusión.

Para empezar este capítulo con un resumen de los siguientes análisis y evaluaciones, se supone que las innovaciones tecnológicas esperadas no sólo permitirán rápidos avances de nuevas micro y nanotecnologías sino también el desarrollo de sensores integrados a gran escala y dispositivos informáticos de nuevas tecnologías de redes y comunicaciones, y de aplicaciones y servicios innovadores. Estas innovaciones permitirán establecer dos direcciones principales de las evoluciones:

- convergencia de los actuales ordenadores y teléfonos móviles de usuario hacia dispositivos de cálculo y comunicación multiuso móviles y portátiles; y
- evolución de la actual Internet y de los servicios y tecnologías web en una futura Internet. La "Internet de los objetos", que vendrá caracterizada por una masiva comunicación y movilidad de los individuos y de todos los tipos de dispositivos y objetos, será un paso adelante hacia una futura Internet eficaz, fiable y segura.

Estos avances tecnológicos se verán reforzados por las demandas del mercado y de los consumidores y desembocarán en el desarrollo de nuevos productos, aplicaciones y servicios de las TIC. De acuerdo a un estudio publicado por Forbes, los sectores de ocio y comunicaciones, de energía y de sanidad pública serán fundamentalmente las fuerzas impulsoras y los principales dominios de aplicación de los nuevos productos de las TIC.[59]

---

[59] Robert Krysiak, "Semiconductor Mega-trends in 2010", Forbes, enero de 2010, www.forbes.com/2010/01/04/stmicroelectronics-healthcare-entertainment-technology-cio-network-semiconductors.html.

A este respecto, los siguiente tres subcapítulos resumirán los principales factores que conformarán los futuros desarrollos de las TIC y sus consecuencias: tendencias tecnológicas, demandas del mercado y del consumidor e "Internet de los objetos", mientras que los dos últimos subcapítulos presentan las posibilidades, amenazas y retos básicos de estas innovaciones en las TIC para nuestra vida pública y privada.

Tendencias tecnológicas

Sin duda alguna, en la década actual, la miniaturización y la digitalización han contribuido de forma significativa al gran paso que se ha dado hacia el "mundo digitalizado" en el que todos los tipos de datos, información y conocimiento se almacenan, transmiten y procesan en forma digital. Los análisis de las tendencias de nuevos desarrollos de sus tecnologías de base actuales, los semiconductores, indican que la ley de Moore ("cada dos años se produce una duplicación del número de transistores por unidad de superficie") probablemente seguirá siendo válida durante al menos otra década. Las actuales técnicas de diseño y fabricación permiten integrar algunos miles de millones de transistores en un solo chip. Incluso aunque a largo plazo las actuales tecnologías de semiconductores sean sustituidas gradualmente por nuevas tecnologías, tales como las biotecnologías o el cálculo cuántico, estas tendencias generales hacia la miniaturización y la digitalización y hacia el aumento de la funcionalidad y la aplicabilidad continuarán y permitirán seguir ampliando las TIC y los productos y aplicaciones basados en las TIC.

A este respecto, en el contexto de los avances del hardware, el software y los microprogramas (firmware), deben considerarse cuatro áreas fundamentales de los futuros desarrollos y principios de organización de los sistemas digitales:

- Sistemas informáticos sencillos y múltiples.
- Redes, protocolos y servicios de comunicaciones.
- Nanotecnologías, ciencias de los materiales, sensores, actores y sistemas incorporados.
- Funcionamiento descentralizado y mecanismos de organización de los sistemas digitales.

Como la integración a muy gran escala de transistores en la superficie de los chips y las frecuencias de reloj cada vez más elevadas crean problemas de sobrecalentamiento, los actuales **microprocesadores** se han diseñado como procesadores multinúcleo que funcionan con frecuencias de reloj reducidas pero con mayor rendimiento gracias al sistema de procesamiento en paralelo en el chip. Mediante las tecnologías de semiconductores multicapas se introducirán más innovaciones en el procesador, lo que aumentará el número de procesadores centrales y disminuirá el consumo de

potencia de cada chip. Ello dará lugar a una mejora significativa del rendimiento mediante procesadores de múltiples núcleos, sistemas de microprocesadores, incremento de las capacidades de memoria caché y principal y desarrollo de sistemas contenidos en un solo chip. Estas tendencias mejorarán el comportamiento de toda la gama de ordenadores, desde los ordenadores de un solo chip e incorporados en los componentes de cálculo hasta los superordenadores. Como también se producirán avances en las redes de comunicación y conmutación, podrá disponerse de todo tipo de estructuras y arquitecturas de ordenadores interconectados.

Además, mediante las técnicas de miniaturización mejoradas, también se dispondrá de dispositivos de almacenamiento externo rápidos, con mayores capacidades de almacenamiento y con tiempos de acceso minimizados. Junto con las técnicas de software y los enfoques arquitectónicos avanzados será posible la ejecución masiva en paralelo de aplicaciones de software complejas. Además, gracias al desarrollo de nuevas tecnologías y el uso de baterías de baja potencia, se mejorará o facilitará la movilidad de los ordenadores y de todos los tipos de dispositivos de cálculo.

En el área de las **redes, protocolos y servicios de comunicaciones**, las innovaciones más importantes se derivarán de las mejoras permanentes de las técnicas de comunicación inalámbrica y por satélite, que ofrecen mayor conectividad y mayores anchuras de banda. Una tendencia de gran importancia se refiere a la formación dinámica de redes virtuales; por ejemplo, redes privadas virtuales[60]. Esta técnica, que ya se aplica, ofrece la oportuna formación y utilización limitadas de aplicaciones y redes orientadas al usuario consistentes en componentes de red y servicios seleccionados.

Otra tendencia hacia una mayor flexibilidad y capacidad de utilización de las actuales infraestructuras informáticas y de comunicaciones se refiere a la formación de redes superpuestas. Hoy en día, como un tema de investigación importante, este enfoque técnico se considera un método eficaz para superar las actuales limitaciones de los protocolos IP/TCP existentes y evolucionar del IPv4 al IPv6, que son pasos importantes para ampliar la utilización de Internet y de "Internet de los objetos". Los avances técnicos en ambos sentidos son requisitos previos para seguir innovando la tecnología de Internet y sus aplicaciones. El enorme crecimiento que ha experimentado Internet, especialmente en lo que se refiere a la variedad y al número de objetos conectados a Internet, requiere por un lado un significativo aumento del actual espacio de

---

[60] James Henry Carmouche, IPsec Virtual Private Network Fundamentals, Cisco Press, 19 de julio de 2006, www.ciscopress.com/bookstore/product.asp?isbn=1587052075.

direcciones de los objetos de Internet (IPv4) hacia IPv6[61]. Por tanto, deben desarrollarse técnicas de transformación especiales que permitan una transición extrapolable entre estas dos normas. Por otro lado, y en paralelo con la evolución de IPv4 a IPv6, debe lograrse el desarrollo de futuros protocolos IP/TCP normalizados para permitir la comunicación entre todo tipo de objetos a través de la "Internet del futuro". Aunque ambas direcciones de investigación requerirán soluciones concretas, puede suponerse que en unos pocos años se utilizarán estas bases técnicas para una futura Internet, ofreciendo capacidades avanzadas y nuevas para las aplicaciones de Internet; por ejemplo, para la "Internet de los objetos".

Además de las tendencias en el desarrollo de sistemas TIC antes mencionadas, deben considerarse los rápidos avances técnicos y de producción en **nanotecnologías, ciencias de los materiales y componentes digitales especializados, como en los sensores, actores o sistemas incorporados basados en semiconductores**, cuando se analicen las futuras tendencias y amenazas de las TIC. Estos avances se traducirán en componentes de las TIC tales como:

- Interfaces de usuario tangibles.[62]
- Pantallas de polímeros.
- Ropa digital (ordenador corporal).[63]
- Sensores activos y pasivos (tecnologías RFID).[64]
- "Ambiente inteligente"[65] o sistemas "inteligentes".

---

61 S. Deering and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", The Internet Society, Dec. 1998, www.ietf.org/rfc/rfc2460.txt; Walter Goralski,, "The illustrated Network: How TCP/IP Works in a Modern Network", The Morgan Kaufmann Series in Networking, 2008, www.freshwap.net/forums/e-books-tutorials/120250-illustrated-network-how-tcp-ip-works-modern-network.html.

62 Hiroshi Ishii, "The tangible user interface and its evolution," Communications of the ACM, Vol. 51, Issue 6 de junio de 2008, http://portal.acm.org/citation.cfm?id=1349026.1349034.

63 Steve Mann with Hal Niedzviecki, Cyborg: Digital Destiny and Human Possibility in the Age of the Wearable Computer, Doubleday of Canada, Nov. 2001.

64 RFID Adoption and Implications, European Commission (Enterprise & Industry Directorate-General, ICT for Competitiveness and Innovation), DG Enterprise & Industry, The Sectoral e-Business Watch, Impact Study No. 07/2008, Final Report, Sept. 2008, www.ebusiness-watch.org/studies/special_topics/2007/rfid.htm;. Arun N. Nambiar, "RFID Technology: A Review of its Applications", Proceedings of the World Congress on Engineering and Computer Science 2009, Vol II, WCECS 2009, 20–22 October 2009, San Francisco, USA, www.iaeng.org/publication/WCECS2009/WCECS2009_pp1253-1259.pdf.

Junto con estos avances técnicos, los nuevos y mejorados mecanismos de organización, **servicios y productos firmware/software** ofrecerán oportunidades para mejorar y añadir funcionalidades y servicios. Estos avances van desde diversas tecnologías de software innovadoras (por ejemplo, desarrollo de software basado en agente), arquitecturas orientadas a servicio (SOA), nuevos servicios web o sistemas de gestión (por ejemplo, para lograr un almacenamiento y recuperación de datos eficaces o para obtener un equilibrio de carga eficiente) hasta la utilización eficaz de infraestructuras de retícula constituidas por grandes redes de ordenadores distribuidos y recursos de comunicación. Las aplicaciones más importantes y de mayor alcance son las de retículas de ordenadores o nube informática[66] que abren una nueva era de las TIC en lo que respecta a sus componentes económicos, de comportamiento, de disponibilidad y de fiabilidad.

Además de todos los avances tecnológicos descritos con anterioridad, deben tenerse en cuenta especialmente dos tendencias fundamentales de gran importancia relativas a los **principios de organización y funcionamiento**, a la hora de analizar las tendencias y amenazas esenciales de las innovaciones en las TIC: **virtualización y descentralización**. El aumento permanente de las funcionalidades y la interconectividad de los componentes digitales heterogéneos, por un lado, y la demanda de su uso efectivo, por otro lado, han desembocado en la constitución y explotación de sistemas virtuales; por ejemplo, procesadores virtuales, de almacenamiento virtual o incluso ordenadores virtuales. Además, el permanente incremento de la complejidad de las redes de ordenadores y de los sistemas de comunicación y la utilización de redes virtuales, como se ha mencionado anteriormente a menudo impiden un funcionamiento eficaz basado en un control centralizado. En lugar de ello, se aplican cada vez más mecanismos de funcionamiento para el control de sistemas descentralizados, lo que ha demostrado ser más flexible y eficaz en comparación con los centralizados. Ejemplos de estos últimos son las aplicaciones de software basadas en agente o el control de sistemas bioanalógicos.

---

65 E. Aarts, R. Harwig, M. Schuurmans, chapter "Ambient Intelligence", in Peter J. Denning, ed., The Invisible Future: The Seamless Integration Of Technology Into Everyday Life, McGraw-Hill Companies, 2001 at 235-250; D. Wright, S. Gutwirth, M. Friedewald et al., Safeguards in a World of Ambient Intelligence, Springer, 2008, www.springer.com/computer/database+management+&+information+retrieval/book/978-1-4020-6661-0.

66 Vladimir Britkov, "Grid and Cloud Computing", Artículo presentado a la Federación Mundial del Panel Científico Permanente para supervisar la seguridad de la información, mayo de 2010 (en adelante "Britkov").

La realización y aplicación de ambos principios juntos, virtualización y descentralización, ya se ha traducido en nuevas oportunidades para un uso eficaz de los recursos digitales interconectados. Tales redes pueden formar "retículas"[67]. Una retícula de ordenadores consta de nodos de ordenadores interconectados, una retícula de datos está formada por sistemas de almacenamiento distribuidos interconectados y las retículas de equipos están constituidas por dispositivos especializados a los que puede accederse a distancia. En el caso de la nube de ordenadores puede accederse a estos recursos interconectados y utilizarlos a distancia a través de los proveedores. Junto a estas ventajas económicas y de comportamiento también deben considerarse algunos riesgos. El desafío más importante, y actualmente el riesgo principal, se refiere a controlar la complejidad de estos sistemas, especialmente en lo relativo a la seguridad y la fiabilidad. Con respecto al estado actual de la ciencia, los sistemas interconectados, que ya están en funcionamiento, no pueden ser ni plenamente verificados con relación a su exactitud ni completamente validados con respecto a aplicaciones específicas ni totalmente probados debido a su enorme tamaño. Esta situación no ha recibido hasta ahora la adecuada atención aunque supone un problema fundamental para las innovaciones de las TIC.[68] Además de este reto, surgen otros riesgos debidos a la aparición de fallos y averías, así como a causa de la posible utilización y manipulación inadecuadas. Estos riesgos deben tener en cuenta una evaluación global de estas innovaciones de las TIC y se requiere urgentemente realizar más investigaciones sobre las contramedidas necesarias.

Tendencias del consumidor y demandas del mercado

Actualmente, una demanda importante de los mercados y los consumidores se refiere al acceso ubicuo al cálculo, la comunicación y la información, lo que significa la utilización de dispositivos digitales y capacidades de interconexión "en cualquier lugar y en cualquier instante". La elevada movilidad de los consumidores, por un lado, y la distribución y disponibilidad global de la información y el conocimiento, por otro, hacen que aumente la demanda de funcionalidades añadidas o mejoradas de los productos TIC y de su empleo eficaz. Estas demandas crecerán y serán generadas de forma permanente y sustancial por diferentes mercados. Por ejemplo, existe una

---

67 Britkov.

68 Vladimir Britkov and Axel Lehmann, "Security challenges arising from innovations in information and communication technologies (ICT),", International Seminar on Nuclear War and Planetary Emergencies, 38th Session. E. Majorana Centre for Scientific Culture, Erice, Italy, 19-24 de agosto de 2007 at 503-515.

demanda cada vez mayor para una cooperación localmente distribuida e independiente del tiempo en las industrias y economías.

Todas estas demandas se basan implícitamente en la hipótesis de que vamos a vivir y trabajar en un mundo completamente digitalizado donde cada objeto individual o cada pieza de información pueden obtenerse y utilizarse en cualquier instante desde cualquier emplazamiento. Estas demandas impulsadas por el consumidor y el mercado generan un "tirón" significativo de las innovaciones tecnológicas; por ejemplo, para utilizar de forma eficaz las aplicaciones multimedios y de vídeo, al acceso ubicuo a la web, el trabajo en grupo asistido por ordenador (CSCW) o el empleo de una gran variedad de servicios y aplicaciones (basados en la web). Además de los componentes y productos TIC nuevos y útiles, los avances hacia la "Internet de los objetos" pueden provocar la aparición de nuevos temas sociales y de gobernanza, así como posibles amenazas a la seguridad. Por tanto, estas innovaciones y sus implicaciones deben analizarse detenidamente desde el principio, lo cual quiere decir desde ahora mismo (véase el siguiente subcapítulo).

Como se ha descrito anteriormente, los actuales y futuros avances en el hardware/firmware/software permitirán nuevos productos basados en las TIC y aplicaciones innovadoras en este sentido y para diversos dominios de aplicación. Como ejemplos de tales dominios de aplicaciones pueden citarse los siguientes:

- Entorno asistido (por ejemplo, para las personas de edad).[69]
- Sistemas de control inteligente (por ejemplo, en transporte, logística, aeronáutica para la navegación, ahorro de energía, etc.).
- Hogares "inteligentes".[70]
- Servicios de asistencia sanitaria.

Si bien las demandas en los sectores de ocio y comunicaciones se centran fundamentalmente en los aspectos de comportamiento y económicos de las TIC, otros

---

69 Kizito Ssamula Mukasa, Andreas Holzinger, Arthur I. Karshmer, "Intelligent User Interfaces for Ambient Assisted Living", Proceedings of the 13th International Conference on Intelligent User Interface, ISBN: 978-1-59593-987-6, 2008, http://portal.acm.org/citation.cfm?id=1378856; Fraunhofer IRB Verlag, ISBN 978-3-8167-7521-8, http://verlag.fraunhofer.de/PDF/English_Publications_2010.pdf.

70 P. Rashidi, D. J. Cook,"Keeping the Resident in the Loop: Adapting the Smart Home to the User," in Systems, Man and Cybernetics, Part A: Systems and Humans, IEEE Transactions, Sept. 2009, Vol. 39, Issue:5 at 949–959, http://ieeexplore.ieee.org/xpl/RecentIssue.jsp?reload=true&punumber=3468; The CASAS Smart Home Project, Washington State University, USA, http://ailab.eecs.wsu.edu/casas/.

dominios de aplicación tales como sistemas de control o vigilancia en los sectores de energía y asistencia sanitaria deben satisfacer los requisitos primarios de seguridad y fiabilidad. Como se ha mencionado en el subcapítulo precedente, el número y capacidades cada vez mayores de los dispositivos digitales utilizados en estas aplicaciones junto con su casi ilimitada interconectividad da lugar a problemas de "explosión del espacio". Se necesita urgentemente realizar investigaciones básicas y aplicadas para desarrollar los adecuados métodos de diseño, verificación y validación, así como para someter a prueba las estrategias que puedan garantizar estos requisitos de calidad.

La "Internet de los objetos"

La "Internet de los objetos" es la idea de que, además de los individuos, todos los tipos de objetos, dispositivos o mercancías de nuestra vida diaria ("objetos") pueden conectarse a través de una futura Internet. Estos "objetos" pueden recibir, almacenar, procesar o emitir datos e información mediante la comunicación con otros "objetos", individuos o servicios. Ello exige que muchos más "objetos" tengan dirección Internet, lo cual será posible con IPv6, y actúen por sí mismos o en subredes como fuente física o punto de acceso para las comunicaciones, la cooperación y el cálculo.[71]

Una implementación gradual de esta visión podría plasmar la idea de "cálculo y comunicación ubicuos" que Mark Weiser expresó hace unos 20 años.[72] Una característica importante de esta visión es el desarrollo de objetos técnicos para convertirlos en "objetos inteligentes" con limitadas capacidades de cálculo y razonamiento y que están conectados a través de Internet con el ciberespacio. Un ejemplo de "objeto inteligente" podría ser un sensor activo que recibe información de otros objetos, procesa esta información y, basándose en su situación actual, reacciona enviando mensajes de respuesta a otros objetos. Esto permitirá establecer la comunicación entre individuos y "objetos", pero también entre los propios "objetos"

---

71 Internet of Things — An action plan for Europe, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, http://ec.europa.eu/information_society/policy/rfid/documents/commiot2009.pdf; "Appendix F: The Internet of Things (Background), Disruptive Technologies: Global Trends 2025, SRI Consulting Business Intelligence, www.dni.gov/nic/PDF_GIF_confreports/disruptivetech/appendix_F.pdf.

72 Mark Weiser, "The Computer for the Twenty-First Century", Scientific American, Sept.1991 at 94-110, www.cim.mcgill.ca/~jer/courses/hci/ref/weiser_reprint.pdf.

ofreciendo oportunidades completamente nuevas para aplicaciones, pero con riesgos respecto a la seguridad de las TI (privacidad, autenticidad y seguridad de los datos).

Amenazas actuales

Como se ha mencionado anteriormente, la escala, complejidad y apertura de nuestro mundo digital interconectado ha alcanzado un nivel en el que no es una sorpresa que los abusos aumenten rápidamente y las tendencias de la futura expansión de las TIC incrementen aún más el número y las posibilidades de amenazas si no se consideran detalladamente.

Existen muchos informes al respecto, ya sea elaborados por las partes interesadas en vender soluciones de seguridad de las TIC, por ejemplo MacAfee[73], Symantec[74] y Kaspersky[75], o por otros interesados que discuten temas de seguridad más generales o que buscan la seguridad de sus propios sistemas y productos TIC.[76] Las categorías de métodos de ciberdelito abordadas en estos informes son las siguientes:

1. **Código malicioso o software pernicioso (malware)**: es un software basado en el intento percibido del creador en vez de en unas características particulares. El malware incluye virus y gusanos informáticos, caballos de Troya, software espía (spyware), anuncios deshonestos, software delictivo (crimeware) la mayoría de los encubridores (rootkits) y otros software maliciosos e indeseados.[77] Symantec informó que entre 2007 y 2008 las nuevas amenazas maliciosas habían aumentado de 624 000 a 1 656 000.
2. **Correo basura (spam)** es el abuso de sistemas de mensajería electrónica (incluidos la mayoría de los medios de difusión y los sistemas de distribución digital) que envían indiscriminadamente grandes cantidades de mensajes no solicitados. La forma más frecuentemente utilizada de spam es el correo electrónico no solicitado con contenido comercial enviado en enormes cantidades. El bajo coste que supone el envío provoca un alto valor potencial. Sin embargo, cada vez con más frecuencia el spam se envía con intenciones

---

73 McAfee Security Advice Center, http://home.mcafee.com/advicecenter/.

74 "Internet Security Threat Report", Symantec, www.symantec.com/business/theme.jsp?themeid=threatreport.

75 Kaspersky, www.kaspersky.co.uk/index.html.

76 "Security Tech Center," http://technet.microsoft.com/en-us/security/default.aspx; SANS, www.sans.org/.

77 Véase esta definición y más explicaciones en: http://en.wikipedia.org/wiki/Malware.

delictivas, con contenido de malware o con la intención de engañar a las personas para que realicen pagos, proporcionen información, etc. (usurpación de identidad).

A fin de ocultar la dirección del remitente y poder enviar una gran cantidad de mensajes, los delincuentes emplean a menudo zombis o robots (ordenadores ajenos que actúan como esclavos a distancia bajo control externo sin el conocimiento del propietario) o redes de zombis (también llamadas redes robot). Se estima que en 2008 se enviaron un total de 350 000 millones de mensajes spam, de ellos el 90% a través de redes robot. Ello supone aproximadamente el 85% del total de mensajes enviados en todo el mundo.

3. Las direcciones web y los servidores de **suplantación de identidad (Phishing)** falsifican o se hacen pasar por direcciones web o direcciones de correo electrónico de entidades dignas de confianza (por ejemplo, bancos) con el intento delictivo de adquirir información sensible tales como nombres de usuario, claves o detalles de las tarjetas de crédito. El malware puede instalarse en un ordenador que enviará al usuario a esa dirección web de suplantación de identidad en vez de a la dirección de confianza correspondiente o puede enviarse spam con direcciones usurpadas que invitan al usuario a hacer clic en un enlace a una dirección de suplantación de identidad. Los informes han detectado unos 55 000 servidores de suplantación de identidad en 2008, lo que supone un 66% más que en 2007.

4. Se están utilizando ordenadores de muchos usuarios para crear **virus y redes robot (bots y botnets)** sin que dichos usuarios sean conscientes de ello. Estos ordenadores se utilizan directamente o se "alquilan" para uso delictivo en el mercado negro. Symantec ha encontrado unos 75 000 ordenadores infectados por robots cada día y 15 197 nuevos servidores distintos de mando y control de robots. Los servidores de economía sumergida proporcionan un mercado negro para la información robada (sobre tarjetas de crédito, ID, etc.) o venta/alquiler de malware o redes de robots.

Si bien generalmente se informa de que la mayoría de los ataques tienen su origen en EE.UU., seguido de Brasil y China, dichos ataques pueden ser lanzados en cualquier instante por cualquier persona, situada incluso en emplazamientos distantes. Aunque el ataque Conficker, basado en una vulnerabilidad del día cero, aún está fresco en nuestra memoria, puede llegarse con precauciones a la conclusión de que el número de vulnerabilidades de día cero está disminuyendo debido a la atención cada vez mayor que se presta a la seguridad de los sistemas de explotación y a las aplicaciones por parte de las grandes empresas de software.

Los intentos delictivos se centran en el sector financiero, que atrae más del 70% de los casos de suplantación de identidad, ocupando los ISP el segundo lugar con sólo el 11%.

El *Whitebook: Emerging ICT Threats* elaborado por el consorcio FORWARD[78] tiene por objeto analizar las nuevas y futuras amenazas de forma sistemática. Define cuatro ejes a lo largo de los cuales se anticipan los próximos desarrollos o los que están teniendo lugar en la actualidad: *nuevas tecnologías, nuevas aplicaciones, nuevos modelos comerciales y nueva dinámica social*. Se identifican 28 amenazas clasificadas en ocho categorías:

1. *Interconexión*: amenazas relativas a la introducción y desarrollo de nuevas tecnologías de red y a los servicios de infraestructura (encaminamiento, DNS) sobre Internet.
2. *Hardware y virtualización*: amenazas debidas a los nuevos desarrollos de hardware y software relativos a la virtualización y a la nube informática.
3. *Dispositivos débiles*: amenazas introducidas con nuevos dispositivos informáticos que son limitadas, tanto en el cálculo como debido a las restricciones de potencia.
4. *Complejidad*: amenazas que surgen debido a la complejidad y escala de los futuros sistemas, que conducen a interacciones de dependencia inesperadas y no intencionadas y a consecuencias en la seguridad.
5. *Manipulación de datos*: amenazas derivadas del hecho de que las personas (y los sistemas) almacenan más datos en línea y estos datos cada vez poseen más valor y son más sensibles.
6. *Infraestructuras de ataque*: amenazas debidas al hecho de que los adversarios desarrollan e instalan de manera activa plataformas de ofensiva (tales como redes robots). Ya no realizan acciones de ataque y huida sino que establecen bases operacionales en Internet para llevar a cabo campañas maliciosas.
7. *Factores humanos*: amenazas debidas a ataques internos, especialmente en el contexto de la contratación exterior, y amenazas referentes a nuevos ataques de ingeniería social.
8. *Requisitos de seguridad insuficientes*: amenazas relativas a sistemas tradicionales y comercialmente disponibles que no han sido concebidos con

---

78 "The FORWARD Emerging ICT Threats Whitebook," www.ict-forward.eu/whitebook/.

suficiente protección y están siendo utilizados e instalados en entornos en los que sus mecanismos de protección son inadecuados.

Esta clasificación permite priorizar los esfuerzos (de investigación) adicionales necesarios para disminuir las amenazas, teniendo en cuenta la severidad, la probabilidad esperada y los actuales esfuerzos desplegados. Se ha llegado a la conclusión de que debe darse la mayor prioridad a las amenazas relativas a: *paralelismo, la escala, las estructuras de soporte económico subterráneas, el malware de los dispositivos móviles y las redes sociales*.

El estado actual de las amenazas es una clara razón de alarma y exige una acción coordinada urgente a nivel mundial por parte de expertos en una cierta variedad de disciplinas, así como por parte de los políticos y diplomáticos. Si bien algunas amenazas requieren fundamentalmente esfuerzos para desarrollar una reglamentación, unas normas, unas técnicas o unas herramientas sobre seguridad evolucionadas o mejoradas, otras exigen urgentemente realizar esfuerzos de investigación científica y encontrar soluciones para su implementación práctica.

Conclusiones

Los futuros desarrollos en investigación y productos de las TIC repercutirán de manera significativa en el comportamiento individual, social y cultural del mundo, tanto en la vida pública como privada. La (r)evolución de los sistemas digitales, de Internet y de sus servicios y aplicaciones se están convirtiendo en recursos básicos para la vida diaria. Este mundo digital ofrece muchas ventajas y posibilidades para la humanidad y los avances técnicos, así como nuevos medios de superar algunos problemas globales como el energético o los cuidados sanitarios. En este capítulo se han considerado las posibilidades y ventajas básicas de las futuras tecnologías y aplicaciones de las TIC.

A pesar de estos aspectos positivos, han aparecido problemas nuevos y de gran calado que requieren una investigación básica intensiva y soluciones adecuadas: el problema fundamental es la ausencia de métodos de diseño y análisis que esté científicamente probado que pueden controlar la enorme complejidad de los futuros sistemas digitales interconectados, especialmente en lo relativo a la fiabilidad, la funcionalidad y la seguridad (privacidad, autenticidad y seguridad de los datos). El desarrollo de soluciones para este problema fundamental es uno de los retos más importantes al que se enfrentan las comunidades de investigación en ciencias informáticas y ciencias de la web. La distribución mundial de una "lista de problemas importantes" abierta como la elaborada por la Federación Mundial de Científicos, junto con el establecimiento de contramedidas eficaces, si se dispone de ellas, podría ser un paso muy útil para lograr este objetivo.

Pero estas medidas no sólo se refieren a las actuales técnicas de diseño y producción. Siempre deben tenerse en cuenta las consecuencias de los errores humanos, los fallos técnicos, las averías o la utilización o manipulación inadecuadas, y deben desarrollarse y aplicarse contramedidas en la medida de lo posible y teniendo en cuenta las restricciones indicadas.

Además, no se dispone de las medidas adecuadas para que los usuarios, los consumidores o las instituciones sean conscientes de los principales problemas, riesgos e incluso amenazas a la hora de utilizar los recursos de las TIC. Los profesionales de los medios de comunicación deben intervenir en el desarrollo de materiales de información sobre temas de seguridad en las TIC dirigidos a diferentes audiencias. Como se ha discutido en el Capítulo II, las sociedades modernas dependen de las TIC y de la evolución de Internet. Por tanto, hay que analizar detenidamente las consecuencias de los futuros desarrollos tecnológicos hacia un mundo digitalizado y deben comunicar los resultados con objeto de crear la confianza necesaria.

4.2 Censura de Internet por los Gobiernos: Ciberrepresión

Por Henning Wegener

La libre expresión de opiniones y el libre acceso a la información constituyen el verdadero núcleo de una sociedad de la información que funciona y son ingredientes esenciales de la ciberestabilidad y la ciberpaz, como se define en el Capítulo VI "Un concepto de ciberpaz" por el mismo autor. Las amenazas a este ejercicio menoscaban o niegan las ventajas fundamentales de Internet y, por tanto, deben considerarse como una de las principales amenazas en el ciberespacio.[79]

La libertad de opinión y el libre acceso a la información han sido a lo largo de la historia elementos clave en la construcción de las sociedades civilizadas. Forman parte indispensable de los derechos humanos y las libertades civiles y constituyen, en consecuencia, piezas centrales de casi todas las constituciones modernas. Evidentemente, la libertad del individuo para adquirir información y mantener y comunicar opiniones puede servir como vara de medir el progreso humano. Por otro lado, la definición de los límites que pueden imponerse a esta libertad fundamental por razones de seguridad pública, decencia y *orden público* siempre han sido un elemento intrínseco de debate político interno y un esfuerzo necesario y permanente en el intento de reconciliar y optimizar tanto la libertad individual como el interés público.

La censura por parte del gobierno sobrepasando sistemáticamente estos límites y ejerciendo un férreo control sobre la opinión pública y el intercambio de opiniones, principalmente respecto al material impreso, es una dolorosa pero recurrente parte de la historia de la humanidad y ha desatado una y otra vez batallas para lograr la libertad de pensamiento.

---

79 La Federación Mundial de Ciéntíficos ha abordado previamente este problema en su contribución a la Cumbre Mundial sobre la Sociedad de la Información (CMSI) en su fase de Túnez 2005. "Seguridad de la información en el contexto de la brecha digital", específicamente en la Recomendación 5 contenida en la misma "Denegación del acceso a la información a través del filtrado de Internet", Pág. 12, y comentarios explicativos Págs. 24-30, www.itu.int/wsis/docs.2/tunis/contributions/co1,pdf, y www.unbiw.de/infosecur. Véase también, con un enfoque similar al del presente capítulo, Henning Wegener "Cyber Repression: Framing the Problem. Assessing the State of Debate and Thinking of Counter-Strategies", in Rights and Responsibilities in Cyberspace. Balancing the Need for Security and Liberty, 2010, EastWest Institute and World Federation of Scientists, www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty.

En la era de Internet esta constelación básica no ha cambiado pero su importancia y la forma que toma sí lo ha hecho. Las tecnologías digitales han catapultado las oportunidades de acceso a la información y la comunicación hacia una nueva dimensión; ello constituye la esencia de la sociedad de la información en la que nos encontramos. Como en cualquier otro aspecto, Internet amplía el alcance, confunde las medidas de cantidad y calidad, niega la distancia y el tiempo y crea nuevos fenómenos ambivalentes.

Internet no sólo incrementa la información y su accesibilidad de forma exponencial sino que también aumenta las posibilidades de intervenir en los procesos técnicos subyacentes y manipular los contenidos digitales. La tecnología digital permite filtrar el software que puede bloquear cualquier área de información, a través de todo Internet o sólo relativa a ciertos servidores, y permite a los gobiernos introducir la censura gubernamental a gran escala. El tema de la libertad de opinión y de acceso a la información como derecho de los seres humanos debe considerarse nuevamente: Internet se está convirtiendo rápidamente en un nuevo campo de batalla en la lucha por los derechos humanos y la libertad de opinión.

Las principales técnicas disponibles para llevar a cabo la censura gubernamental son el bloqueo de IP, el filtrado y redireccionamiento del DNS, el filtrado de URL mediante la exploración de las palabras clave objetivo, o el filtrado de paquetes, que consiste en la terminación de la transmisión de paquetes de TCP una vez detectadas las palabras clave controvertidas. Una característica es que el actual software de filtrado reacciona sólo mecánicamente a la aparición de ciertas palabras o frases y, por consiguiente, sobrepasa el objetivo ("sobrebloqueo").

El número de suministradores industriales de software de filtrado que utilizan éstas y otras técnicas es enorme. Incluyen la mayoría de las principales empresas de tecnología de la información pero también empresas especializadas. Existen varias páginas web dedicadas a evaluar comparativamente y a clasificar tales ofertas de software con relación a su eficacia mientras que otras páginas explotadas por partidarios de la total libertad de expresión en Internet critican la simple aparición de esta tecnología.

La tecnología de filtrado debe considerarse conjuntamente con las opciones de puenteado. Esa misma sofisticación que ha marcado el desarrollo de filtros también caracteriza las tecnologías diseñadas para evitar, puentear o dañar los filtros. La censura total de la información en Internet es muy difícil o incluso imposible de lograr debido a la tecnología distribuida subyacente de la red. Por tanto, hay un cierto número de recursos y soluciones que permiten a los usuarios evitar la censura en Internet. La mayoría de ellos se basan en lograr el acceso a una conexión de Internet

que no esté sometida a filtrado, a menudo situada en una jurisdicción distinta no sometida a las mismas leyes de censura. El reto evidente de los responsables del gobierno de censurar Internet es que mientras exista en el mundo *un* sistema accesible público sin censura, siempre será posible acceder al material sin censurar. Las técnicas disponibles para este acceso clandestino incluyen la utilización de servidores de proximidad, el establecimiento de redes privadas virtuales y la descarga de software de fuente abierta que permita una navegación, comunicación y transferencia de ficheros anónimas (como ejemplos pueden citarse Psiphon, I2P y Tor).

El filtrado del contenido también desempeña una importante función de protección en la sociedad. El bloqueo de páginas de pornografía infantil y la incitación a la violencia, al odio y al crimen racial en general parece gozar de una legitimidad universal y lo mismo cabe decir de todos los medios utilizados para evitar el empleo cada vez mayor de Internet por el terrorismo nacional e internacional. El contenido que no pueda difundirse legalmente *fuera* de Internet debe ser susceptible de sanciones jurídicas y de prohibición también *dentro* de la Red. A este respecto la industria del software de filtrado cubre una necesidad legítima.

Pero en este caso debe hacerse una importante distinción.

Cualquiera que sea la eficacia de los filtros, y por lo tanto el efecto de censura, y cualesquiera que sean los intereses comerciales implicados, es decisivo el hecho de que en las sociedades "libres" principalmente, pero en modo alguno de forma exclusiva, de las llamadas democracias occidentales con su alto grado de consenso en los valores fundamentales, las restricciones en la libertad de expresión y el acceso a la información vienen claramente reguladas por ley, su alcance está controlado por las reglas de pertinencia y proporcionalidad y pueden evaluarse mediante procedimientos jurídicos públicamente accesibles. La existencia de un claro marco jurídico y la disponibilidad de un control jurídico independiente son, evidentemente, los criterios decisivos para distinguir entre el control legítimo del contenido y la censura ilegal; también proporcionan el instrumento para acomodar las diferencias en valores culturales y definiciones de privacidad. El contenido ofensivo para la cultura, la religión, la moral y otras creencias colectivas profundamente arraigadas en ciertos países no deben estar exentos de control bajo el pretexto de lograr una absoluta libertad en Internet y los que denuncian legítimamente esta censura política gubernamental deben ser prudentes a la hora de tomar partido en estos temas.

Como el filtrado de Internet por parte de los gobiernos, los límites a la restricción de la libertad de expresión que deben observarse, los equilibrios que deben establecerse y el cometido de la industria de la TI a la hora de proporcionar las bases técnicas para el

control de Internet son temas todos ellos delicados que pueden afectar a la soberanía nacional, este artículo evita apuntar cualquier responsabilidad sobre cualquier gobierno en concreto; de hecho, no se menciona a ningún país. Igualmente, tampoco se nombra a ningún proveedor de hardware, software o servicios de las TI. Evidentemente, el objetivo del artículo es enmarcar el problema y evaluar el estado del debate y no precipitarse en la obtención de soluciones. En ese mismo espíritu de contención, las citas a páginas web o a otros artículos se hacen únicamente a título de referencia y no implican que este artículo se identifique o apoye su contenido.

Dado el carácter sin fronteras de Internet, la reglamentación nacional no es suficiente para administrar la libertad de Internet. De esa forma, la Unión Europea ha establecido desde 1999 un régimen válido en la UE para regular el acceso admisible al contenido de Internet así como los procedimientos pertinentes ("Programa de Internet más seguro"). Se basa fundamentalmente en el principio de autorregulación por la industria de Internet y mecanismos de búsqueda para excluir los contenidos ilegales o dañinos y garantizar la conformidad con la legislación nacional. En algunas áreas, esta autorregulación funciona satisfactoriamente aunque en algunas ocasiones pueda ser necesaria cierta legislación complementaria.

De forma general puede decirse que las normas jurídicas internacionales vienen determinadas en particular por los dos grandes tratados sobre derechos humanos redactados en los primeros años de existencia de las naciones Unidas: la *Declaración Universal de Derechos Humanos (1948)* y el *Pacto Internacional de Derechos Políticos y Civiles* de 1966. Prácticamente todas las naciones han firmado y ratificado estos textos que se consideran actualmente una ley consuetudinaria internacional que vincula igualmente a los Estados no signatarios. Por pura coincidencia, en ambos documentos es el Artículo 19 el que establece el reconocimiento del principio de libertad de expresión y de opinión, que incluye el derecho que tienen todas las personas a recibir y distribuir información de todo tipo, independientemente de las fronteras y a través del medio elegido. No hay duda alguna de que ello también incluye le recepción de información a través de Internet y el derecho de acceso a la misma (así como el derecho de *impedir* al acceso), y por consiguiente la Cumbre Mundial sobre la Sociedad de la Información (CMSI, 2003 y 2005) confirmó solemnemente estos principios como pilares centrales e indispensables de la sociedad de la información, específicamente en la *Declaración de Principios de Ginebra* (Principios 4, 5 y 55). Conviene señalar que el texto de la CMSI destaca el aspecto de la libertad, disminuyendo las advertencias incluidas en el Pacto Internacional.

Lo que en las sociedades "libres" queda reducido a un difícil problema de equilibrio político permanente entre la libertad y la intervención del Estado bajo claros criterios legales, en muchos otros Estados se ha convertido en un problema de derechos

humanos y de la calidad del orden de la información global. La censura de Internet por parte de los gobiernos a través de tecnologías de filtrado sin restricciones legales y con graves y profundas consecuencias para las personas que buscan y difunden información, constituye una violación de los derechos humanos de gran dimensión. Un componente problemático de este desarrollo es que las empresas tecnológicas occidentales no sólo proporcionan su tecnología de filtrado a los gobiernos que desean imponer la censura sino que también colaboran en su empleo, estableciendo de esa forma unos sistemas de censura eficaces y eficientes. Este fenómeno es fundamental para el presente análisis, que también tiene por objeto sugerir diversas posibilidades de adopción de medidas internacionales contra estas prácticas. Como ha señalado Jo Glanville, editor de "Index of Censorship"[80], "Por primera vez en la historia la censura se ha convertido en una empresa comercial".[81]

Esto se ha escrito en una época en que puede observarse un proceso de crecimiento crítico tanto en el número de gobiernos que practican la censura a Internet, principalmente en detrimento de las libertades y los derechos políticos, como en la capacidad de las técnicas de filtrado.

El estado y desarrollo de la censura de Internet por los gobiernos está supervisada por muchas instituciones privadas, incluida la Precursora Iniciativa OpenNet, Reporteros sin Fronteras y, utilizando a menudo datos y clasificaciones iguales o similares, el Informe de Censura en Internet.[82]

Estas fuentes han observado unánimemente un proceso de crecimiento de la censura de importantes proporciones. Basándose en listas y cifras de sus propios países, llegan a la conclusión de que en la actualidad 1 720 millones de personas resultan afectadas

---

80 Index on Censorship es una prominente organización británica que promueve la libertad de expresión www.indexoncensorship.org..

81 Jo Glanville, "The big business of net censorship", The guardian, 17 nov. 2008, www.guardian.co.uk/commentisfree/2008/nov/17/censorship-internet.

82 OpenNet Initiative, www.opennet.net. El proyecto emplea una red internacional de investigadores para determinar la amplitud y el carácter de los programas de filtrado por Internet llevados a cabo por los gobiernos. Las instituciones académicas participantes incluyen el Centro para Estudios Internacionales de la Munk School de Asuntos Mundiales de la Universidad de Toronto, el Centro Berkman para Internet y la Sociedad de la facultad de Derecho de Harvard, el Instituto de Internet de Oxford de la Universidad de Oxford y el Grupo SecDev que se hizo cargo de los trabajos del Grupo de Investigación Avanzada sobre Redes del Programa de Seguridad de Cambridge de la Universidad de Cambridge. Véase también www.chillingeffects.org donde figura un grupo aún más amplio de instituciones académicas participantes que "controlan el clima jurídico de las actividades de Internet".

por la censura a Internet. Ello supone aproximadamente el 25,3% de toda la población mundial.

La lista de Estados que llevan a cabo estas prácticas es larga. Al menos 25 gobiernos, y probablemente más de 30, impiden a sus ciudadanos la posibilidad de acceder a la gama completa de información disponible en línea. Internet proporciona varias listas de organizaciones que supervisan a estos países. La iniciativa OpenNet clasifica la censura como Total, Sustancial, Nominal e Indirecta, y también mantiene una categoría de Observación. Reporteros sin Fronteras ha elaborado una lista de 13 "Enemigos de Internet". La mayoría de los países controlados centran su intervención en la prohibición del contenido político (libertad, democracia, elecciones libres, recursos jurídicos, informes sobre acontecimientos políticos sensibles, etc.) que su propio sistema de gobierno no permite, pero muchos van más allá. Algunos gobiernos concentran sus restricciones en temas morales y en su orden cultural y moral heredado. La intensidad y profundidad del control varía. En algunos países la censura bloquea las páginas pero desvía la consulta a una página explicativa proporcionando el acceso correspondiente si se demuestra un interés especial "legítimo" en esa información, permitiendo de esa forma un cierto grado de transparencia. En otros países, la censura se practica de forma esporádica e ineficaz y no se aplican sanciones en caso de ruptura del bloqueo.

Como regla general, sin embargo, la censura por parte del gobierno se ejerce sin límites y sobre un amplio segmento del conocimiento humano, sin que haya ninguna explicación o justificación para actuar de esa manera, incluso por parte de países respetables: cuanto más se aleje la forma de gobierno de una democracia al estilo occidental mayor incidencia tiene la censura a través del filtrado de Internet. Algunos Estados llegan a tutorar a su población a través de la censura de Internet hasta extremos grotescos: los usuarios de Internet convictos de acceder a páginas prohibidas son castigados y en algunos países son perseguidos por una ciberpolicía especialmente agresiva. El número de usuarios encarcelados, por los datos que se tienen hasta el presente, es alarmantemente elevado desde cualquier punto de vista. Algunas empresas internacionales de TI que proporcionan software viven con la sospecha de ayudar e incitar tales medidas de represión, contribuyendo así al sufrimiento humano resultante.

Las consecuencias de una censura completa son graves y no deben subestimarse. No sólo se despoja a los ciudadanos de sus derechos con arreglo a las leyes internacionales sino que se les impide acceder a las ventajas que proporciona la incorporación a la era de la información, reciben una visión sesgada e irreal del mundo y su participación en los procesos de enriquecimiento de la comunicación global disminuye. El filtrado masivo de Internet puede alterar el estado mental colectivo de

una nación. También debe tenerse en cuenta el efecto negativo *doble* de esta censura: se priva a los ciudadanos de información y de una visión libre del mundo y es una herramienta para la represión política restringiendo la libertad de acción.

El estado de la situación y el empeoramiento de los casos de censura de Internet exigen una respuesta inmediata. La UE ha reconocido esta situación y está tomando medidas al respecto. No acepta que los gobiernos represivos sean asistidos por empresas de TI para arraigar su dictadura mental. También debemos a la UE el haber acuñado el término, muy apropiado, de "ciberrepresión" para referirse a estas prácticas.

La UE no está sola en esta lucha. El grupo de presión de Internet internacional que se esfuerza para lograr la libertad de información y la integridad de Internet en todo el mundo está activo y vigilante, incluso va más allá que muchas instituciones prominentes ya mencionadas que supervisan el desarrollo de la ciberrepresión y la denuncian públicamente.

Teniendo en cuenta la habilidad de los usuarios experimentados de Internet a la hora de evitar los filtros, muchos defensores internacionales de la libertad de Internet también se han comprometido a proporcionar a los ciudadanos que viven en países donde se ejerce la censura el correspondiente software para contrarrestar dicha censura, como se ha descrito anteriormente. Estas tecnologías antifiltro se han convertido igualmente en una verdadera industria que ayuda a disminuir la eficacia de la censura impuesta por los gobiernos, sin que lleguen a eliminarla completamente. La Iniciativa OpenNet, al igual que otras, es muy activa en este campo y suministra sistemas de eficacia probada (como Psiphon) diseñados para permitir que un ordenador doméstico comercial actúe como un servidor personal de proximidad para encriptación evitando los "cortafuegos" obligatorios introducidos por el gobierno y permitiendo una libre navegación en la red global. Sin embargo, la aplicación de este dispositivo y otros similares está recibiendo la oposición de ciertos suministradores de filtros. Ello demuestra nuevamente el carácter problemático de las actividades comerciales de las industrias multinacionales que, intencionadamente o como efecto colateral no deseado, facilitan o ayudan a la ciberrepresión. Evidentemente, cabe señalar que los países avanzados en las tecnologías digitales pueden desarrollar internamente filtros y muchos ya lo están haciendo, lo que deja descolgados a los proveedores de software extranjeros.

Como se ha señalado anteriormente, este artículo no tiene por objeto realizar un análisis detallado de la situación país por país, teniendo además en cuenta que Internet ofrece una amplia información al respecto. Pero incluso el breve resumen que aquí aparece y el debate público suscitado plantean la cuestión de la evidente

necesidad de tomar medidas al respecto y qué pasos debe dar la comunidad internacional para contrarrestar la ciberrepresión que viola constantemente las leyes internacionales.

Los problemas jurídicos y políticos implicados en la definición de los límites internacionalmente aceptables sobre el filtrado de Internet y las posibles sanciones son evidentes y de gran calado. Las cuestiones relativas a la jurisdicción y soberanía nacionales, la casi imposibilidad de establecer unas fronteras válidas y ampliamente aceptadas entre libertades civiles y violación del interés público, las cuestiones de elección, la ley y los medios para forzar su cumplimiento y el amplio tema del gobierno de Internet, entre otras cosas hace inviable y probablemente inútil todo intento de codificación a nivel internacional. También se plantea la cuestión de la diversidad cultural y el respeto que los demás se merecen. La definición de *orden público* cultural y religioso no puede ser uniforme en todos los países, aunque puede suponerse legítimamente que existe un marco universal de convicciones básicas compartidas y el Pacto Universal de Derechos Humanos debe considerarse vinculante en todo el mundo. Como suele suceder en las leyes internacionales, no existen definiciones fáciles ni sanciones rápidamente eficaces.

Cualquier reforma del filtrado de Internet global debe considerarse en *términos del proceso* y de las *estrategias a lo largo del tiempo*. Debe pensarse en términos de procedimientos que despierten la conciencia en el mundo, generen la sensibilidad y presión públicas adecuadas y, para los gobiernos afectados, supongan un reto para la opinión pública que motive la publicación de justificaciones detalladas.

Una importante responsabilidad recae en los gobiernos y la industria nacionales y en las instituciones de la sociedad civil con su gran poder para crear opiniones. Los gobiernos pueden promover el desarrollo y la disponibilidad de tecnologías antifiltros, pueden someter la exportación de tecnologías de filtrado a los adecuados controles de exportación y pueden utilizar los canales diplomáticos nacionales a fin de ejercer presión sobre los gobiernos que practican la censura, en interés de la transparencia y para que pongan al descubierto y justifiquen sus políticas restrictivas.

La industria de las TI, productores de software y empresas que proporcionan servicios de ISP y sus asociaciones, son claramente responsables y deben proceder a adoptar códigos de conducta que excluyan el empleo de sus tecnologías para ejercer la censura política. Si bien de forma realista no puede pedirse a las empresas que dejen aparte sus intereses comerciales y sería absurdo trasladar a las empresas la responsabilidad principal de la censura ejercida por los gobiernos, la acción colectiva voluntaria por parte de las empresas también puede aumentar su reputación y mejorar la imagen positiva de las mismas. La política de autorregulación, que proporciona una norma

común clara, ha dado buenos resultados en la UE y también puede fortalecer el poder de resistencia de las empresas para soportar las presiones a las que se ven sometidas por parte de los gobiernos que quieren ejercen la censura para hacer negocio con ellos. Como ejemplo, la Iniciativa Red Mundial, que es un esfuerzo voluntario llevado a cabo por las empresas tecnológicas de EE.UU., prescribe tales normas ("Carta de Gobernanza"), reacciona a las solicitudes de los gobiernos para ejercer la censura y promueve la libertad de Internet.[83]

Las instituciones académicas y las organizaciones de derechos humanos que denuncian incansablemente la ciberrepresión, algunas de las cuales se han citado anteriormente, son estimuladas y favorecidas cada vez en mayor medida por los gobiernos que han abrazado su causa. No obstante, teniendo presente el carácter transfronterizo e internacional de Internet y la relevancia mundial que tiene para los derechos humanos la ciberrepresión, la tarea más importante puede que sea introducir este tema en la agenda de las organizaciones internacionales.

Un primer paso podría consistir en llegar a un amplio acuerdo internacional sobre el desarrollo y las bases técnicas del actual filtrado de Internet y sobre la creación de un mecanismo internacional de supervisión.

En una segunda etapa, puede pensarse en la introducción de un procedimiento de quejas internacional ampliamente accesible a todos los interesados y que siga un cierto número de pasos para informar sobre el caso.

¿Qué organismo u organización internacional puede llevar a cabo esta tarea?

En primer lugar, puede pensarse en el Foro sobre el Gobierno de Internet (FGI) creado en 2006 con arreglo a las decisiones de la CMSI ("Agenda de Túnez"). Las restricciones que la censura política de Internet impone al funcionamiento y gestión de la red revisten una importancia evidente para la Asignación del Foro y podría incluirse fácilmente este tema en su mandato (Art. 72 a), b), e) y k) de la Agenda de Túnez), aunque el problema de la ciberrepresión no sea explícitamente mencionado en estos textos. Lamentablemente en sus cinco años de existencia el FGI se ha limitado a celebrar discusiones interesantes y significativas, incluidas algunas de ellas sobre la libertad de Internet, pero no ha llevado a cabo hasta la fecha ninguna actividad operativa. El establecimiento de un procedimiento de supervisión en el que podrían seguirse, analizarse y evaluarse críticamente las prácticas de filtrado sería posible y deseable bajo el mandato del Foro, si se amplía dicho mandato como parece

---

83 Global Network Initiative, www.globalnetworkinitiative.org.

probable.[84] (El foro anual de la CMSI, por el contrario, es un foro de debate abierto sin ninguna asignación operacional y sería menos adecuado para este propósito.)

La UNESCO se proclama a sí misma orgullosamente, bajo su acta fundacional, como la única organización que actúa como guardián internacional de la libertad de información y ha recibido de la CMSI tareas concretas bajo los epígrafes "Acceso a la Información y el Conocimiento" y "Dimensión Ética de Internet". La UNESCO ha adoptado Declaraciones y Recomendaciones que comprometen a los Estados Miembros y a las organizaciones internacionales a facilitar el acceso libre y sin obstáculos a Internet[85] y su Director General no ha cesado de denunciar públicamente violaciones a la libertad de información y de prensa. Nada sería más lógico que iniciar en cumplimiento de estas tareas un diálogo y, como resultado, un examen periódico de las prácticas de censura.

Como se trata de un tema de derechos humanos y se han abordado los dos pactos básicos internacionales que establecen las respectivas obligaciones de los Estados, los foros principales para tomar medidas al respecto deben ser las organizaciones especiales de derechos humanos establecidas en el seno de la Naciones Unidas, el Consejo de Derechos Humanos creado en 2006 y la organización especial para tratar las violaciones del *Pacto Internacional de derechos civiles y políticos.* El Consejo de Derechos Humanos, con su amplio mandato, sería el órgano adecuado para poner en práctica un procedimiento de queja formal disponible a todos los gobiernos miembros

---

84 Al menos el FGI ha demostrado que el tema de la censura no es ajeno al desarrollo de sus trabajos. Durante el actual debate sobre la continuación de las actividades del Foro y una posible amplificación de su mandato, se han hecho propuestas para un mayor diálogo sobre la libertad de expresión y para prestar más atención al desarrollo y la dimensión de los derechos humanos del Gobierno Internacional. Véase el documento A/65/78 de la Asamblea General de las Naciones Unidas (E/2010/68) de 7 de mayo de 2010.

85 "Declaración sobre los principios fundamentales relativos a la contribución de los medios de comunicación de masas al fortalecimiento de la paz y la comprensión internacional, a la promoción de los derechos humanos y a la lucha contra el racismo, el apartheid y la incitación a la guerra". Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, 28 de noviembre de 1978. http://portal.unesco.org/en/ev.php-URL_ID=13176&URL_DO=DO_PRINTPAGE&URL_SECTION=201.html: "Recomendación sobre la Promoción y el Uso de Plurilingüismo y el Acceso Universal al Ciberespacio". Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, 15 de octubre de 2003, http://portal.unesco.org/ci/en/ev.php-URL_ID=13475&URL_DO=DO_TOPIC&URL_SECTION=201.html (que aboga por el "acceso universal a Internet como medio para promover el ejercicio de los derechos humanos definidos en los Artículos 19 y 27 de la Declaración Universal de Derechos Humanos").

de las NU. Una posibilidad sería introducir el tema de la libertad de Internet y su censura obligatoriamente en el proceso de Examen Periódico Universal donde se revisan las estadísticas relativas a los derechos humanos en todos los países. Cualquiera que sea el procedimiento elegido, el hecho de destacar de manera colectiva los abusos de los derechos humanos en esta esfera generaría una sana presión en los gobiernos sospechosos de ilegalidad al respecto y les obligaría a argumentar adecuadamente sus posiciones. En el procedimiento de queja, el dudoso papel de la industria internacional de las TI a la hora de instrumentalizar la ciberrepresión quedaría claramente puesto en evidencia. Como en el ACNUR, el examen periódico de los países en la Comisión de Derechos Humanos de las NU podría incluir también el tema de la libertad de Internet.

Por muy ineficaces que fueran estos dispositivos procedimentales, un régimen totalmente transparente al respecto que desemboque en una presión pública o en una condena generalizada, podría preparar el camino hacia una mayor sensibilización sobre el problema a escala mundial y mejoraría el comportamiento general del mundo digital.

5 Ciberconflicto y estabilidad geocibernética

5.1 Ciberconflicto

Por Giancarlo A. Barletta,[86] William A. Barletta,[87] Vitali N. Tsygichko[88]

Introducción: La naturaleza del desafío

La guerra de la información es tan antigua como el conflicto humano. Los motivos que la generan han cambiado poco; incluyen socavar la confianza del adversario, dañar y crear confusión en las líneas de comunicación del adversario, y engañar acerca de la naturaleza y el contexto del conflicto. Estas motivaciones se han mantenido. Lo que resulta muy innovador en el siglo XXI, una época en que dominan las infraestructuras de información y electrónicas con una profusión de enlaces digitales de gran anchura de banda, es: a) la virulencia y frecuencia de los ataques cibernéticos que pueden perjudicar al tejido social del país objeto de los mismos; b) un enorme potencial para causar grandes daños materiales; c) la capacidad de contagio y la capacidad de actores no gubernamentales e incluso privados, que ahora pueden participar en conflictos bélicos asimétricos, para efectuar ataques cibernéticos sostenidos; y d) la perpetuación de un estado subyacente y generalizado de conflicto de baja intensidad – lo que cabría designar con el nombre de "ciberguerra fría". La introducción intensiva de nuevas tecnologías informáticas ha incrementado de manera considerable las capacidades de combate de los armamentos convencionales y de otras tecnologías militares. Por este motivo, los militares consideran hoy que las tecnologías de la

---

86 Global Cyber Risk, LLC; Washington, DC, Estados Unidos.

87 Massachusetts Institute of Technology, Cambridge, MA, Estados Unidos.

88 Instituto para el Análisis de Sistemas, Academia de Ciencias de Rusia, Moscú, Federación de Rusia.

información y la comunicación (TIC) son a la vez armas y objetivos, y consideran el ciberespacio como un campo de batalla similar al aire, el espacio, la tierra y el mar.[89]

A lo largo de los dos últimos decenios, los países industrializados han implantado redes de activos económicos, físicos y sociales conectadas a través de las TIC, a fin de mejorar su nivel de vida, su prosperidad económica, su influencia y su poder en el ámbito internacional. Del mismo modo, los países en desarrollo consideran a la tecnología de la información como una vía rápida para lograr la plena participación en la economía mundial. Abundan los aparatos inteligentes (que contienen tanto sensores como microprocesadores) destinados a la industria, al igual que ocurre con los aparatos de consumo dotados de microprocesadores y capacidad inalámbrica (o celular) como los teléfonos móviles, las PDA y los notepad electrónicos. La generalización de las redes de comunicación permite la aplicación intensiva de recursos informáticos para propiciar el comercio, prestar servicios, vigilar el medio ambiente y abordar complejos problemas sociales. Todos estos aparatos se están desarrollando rápidamente y cuentan con la capacidad para comunicarse con otros aparatos situados en cualquier lugar del mundo.

Como señala un antiguo General de las fuerzas armadas de los Estados Unidos, las mismas TIC que sirven para conectar los principales activos económicos, materiales y sociales han sido adoptadas y adaptadas por los movimientos militares y cuasi militares, contribuyendo así a una revolución en el terreno militar que está cambiando la manera de planificar, organizar y dirigir la guerra. Esta "revolución" conlleva el desarrollo de la capacidad para llevar a cabo labores de inteligencia, vigilancia y reconocimiento; para mandar y controlar las fuerzas y las operaciones que éstas llevan a cabo; para lograr movimientos logísticos óptimos; para permitir la navegación de precisión y para el empleo de armas "inteligentes". Y lo que es más importante,

---

89 Por ejemplo, "La misión de la Fuerza Aérea de los Estados Unidos es proporcionar opciones soberanas para la defensa de los Estados Unidos de América y sus intereses a nivel mundial—volar, combatir y ganar en el espacio aéreo y en el ciberespacio". "Air Force Strategy: Sovereign Options for Securing Global Stability and Prosperity". 26 Mar. 2008, Office of the Secretary of the Air Force, www.stormingmedia.us/98/9868/A986884.html. La perspectiva estadounidense se desarrolla con más detalle en *Information Operations, Electronic Warfare and Cyberwar: Capabilities and Related Policy Issues*, Congressional Research Service (CRS) Informe, RL31787, 14 de septiembre de 2006, www.fas.org/irp/crs/RL31787.pdf (en adelante "Informe CRS").

también permite la utilización de la "red" como un medio a partir del cual, a través del cual y en el cual llevar a cabo operaciones militares.[90]

Las tecnologías de la información permiten y propician nuevas relaciones inesperadas en el seno de las sociedades, con un potencial natural para mejorar el crecimiento económico, lograr avances en materia de derechos humanos y dar a conocer la represión gubernamental. Las autoridades nacionales disponen de una comunicación vertical descendente muy mejorada pero, lo que es más importante en lo que respecta a la expansión de los derechos humanos y el bienestar económico, los flujos de información ascendentes y horizontales se han convertido en auténticos ríos. En las modernas sociedades de la información se aumentan continuamente tanto el número y los atributos de los nodos de información (allí donde la información se genera y se consume) como el número y el ancho de banda de los enlaces. Por otra parte, un porcentaje creciente de los nodos y los enlaces incluye sensores autónomos para determinar su situación operativa.

Esta enorme conectividad no lineal incrementa de manera simultánea tanto la resistencia de la red informática y los riesgos y consecuencias de los ataques que debilitan los nodos y los enlaces medulares como las dificultades para anticipar las consecuencias de las averías que se producen en la red. La rápida evolución de las TIC y la consiguiente evolución de la sociedad mundial de la información entrañan la posibilidad de engendrar una amplia gama de implicaciones geopolíticas negativas: una aceleración de la polarización mundial entre naciones ricas y pobres, una brecha tecnológica creciente entre los países altamente industrializados y los países en desarrollo, dejando en la cuneta de la evolución de la civilización a un número creciente de países económicamente marginados – un terreno abonado para la inestabilidad política y los conflictos. En consecuencia, a medida que la complejidad de las redes informáticas evoluciona orgánicamente, la posibilidad de guerra informática se desarrolla de una manera que supone un riesgo creciente para los valores sociales.

La proscripción pública de los ciberataques frente a la guerra electrónica encabezada por los gobiernos

Los ataques contra las redes y sistemas informáticos y contra los datos digitales han dado lugar a la promulgación de leyes sobre el ciberdelito en numerosos países. Aunque la mayoría de los países industrializados dispone de algún tipo de legislación

---

[90] General John Casciano, "Threat Considerations and the Law of Armed Conflict", agosto de 2005 (archivado junto con WFS Information Security PMP).

sobre el ciberdelito, las importantes diferencias en cuanto a la definición de lo que constituye un ciberdelito, la detección e identificación del comportamiento criminal en el ciberespacio, y en lo que respecta a las disposiciones sustantivas y de procedimiento aplicables han entorpecido de manera importante la cooperación internacional para la prestación de asistencia en las investigaciones de los ciberdelitos. La Convención del Consejo de Europa sobre Ciberdelito se elaboró como un acuerdo multilateral destinado a iniciar la armonización de la legislación mundial en materia de ciberdelito. La realidad dista mucho, no obstante, de las expectativas. A mediados de 2010, casi nueve años después de que quedara abierta a la firma, tan sólo 26 países habían ratificado la Convención del Consejo de Europa. El Conjunto de herramientas de legislación sobre ciberdelito preparado por la UIT se ha elaborado como una vía alternativa dotada de mayor flexibilidad, ya que facilita ejemplos de lenguaje jurídico armonizado con la Convención del Consejo de Europa y la legislación sobre el ciberdelito de los países industrializados, y pueden utilizarla todos los países del mundo para elaborar o modificar su propia legislación en materia de ciberdelito.

Otras leyes relativas a determinados tipos de ciberactividades incluyen aquellas que se destinan a proteger los sistemas y equipos físicos de los proveedores de comunicaciones, las disposiciones por las que se prohíben los actos de espionaje económico, las leyes de propiedad intelectual, etc. En conjunto, estas leyes están destinadas a establecer una proscripción legal de distintos tipos de ciberataques contra todo tipo de infraestructuras, sistemas y datos.

La ya amplia gama de posibilidades se hace cada día mayor con la aparición de tecnologías de la información más poderosas y de uso generalizado. No cabe extrañarse de que las naciones se sientan muy motivadas para codificar la conducta en el ciberespacio, cualquiera que sea su propio comportamiento respecto de otras naciones. Dado que las tecnologías de la información permiten saltarse con facilidad las fronteras internacionales, los criminales no tienen nunca necesidad de entrar en el estado en que reside la víctima. En consecuencia, los incentivos para la cooperación entre los Estados-nación deberían ser importantes, especialmente si se tiene en cuenta que los recursos informáticos estatales representan un objetivo atractivo para el comportamiento criminal. En efecto, la cooperación tanto para promover una colaboración fructífera en y a través de las redes informáticas como para evitar o, al menos, desalentar la mala conducta en el ciberespacio se ha convertido en una cuestión que reviste interés para los organismos de naturaleza internacional tales como la UIT.

Dado que los gobiernos recurren cada vez más a la Internet para facilitar la distribución de información y servicios a sus ciudadanos, la sociedad de la información aparece como un objetivo tentador para los malhechores, ya sean delincuentes,

grupos terroristas locales o Estados-nación hostiles. El ataque a la infraestructura nacional de información de Estonia en abril de 2007[91] demuestra claramente tanto la prevista vulnerabilidad de un cibergobierno como la falta de elementos de disuasión para el atacante. Muchos expertos han afirmado que la sofisticación técnica del ataque superaba la de otros incidentes anteriores conocidos. Mientras que algunos van hasta afirmar que se requería el conocimiento o la complicidad de una entidad nacional, varios expertos estadounidenses han descartado tal especulación. Sin embargo, debe señalarse que el episodio de Estonia no estuvo acompañado de demandas políticas o económicas ni de manifiestos por parte de los supuestos perpetradores del ataque,[92] por lo que es poco probable que se tratara de criminalidad sin motivaciones políticas. Los ataques experimentados en 2009 por GhostNet[93] y Aurora ofrecen otros ejemplos de ciberataques más sostenidos y generalizados. Uno de los aspectos de los ataques se centró en los servidores de Google, como parte de un esfuerzo concertado de espionaje político y empresarial que "explotaba los fallos de seguridad en los documentos adjuntos a correos electrónicos

---

91 Se ha informado ampliamente acerca del ataque en la prensa internacional. Por ejemplo, *véase* Ian Traynor, "Russia accused of unleashing cyberwar to disable Estonia", *The Guardian*, 17 de mayo de 2007, www.guardian.co.uk/world/2007/may/17/topstories3.russia.

92 A comienzos del mes de junio, un dirigente del grupo juvenil ruso partidario de Putin, Nashi, se había atribuido el ataque. www.rferl.org/content/Russian_Groups_Claims_Reopen_Debate_On_Estonian_Cyberattacks_/1564694.html . Se desconoce la veracidad de esta declaración.

93 *Tracking GhostNet: Investigation of a Cyber Espionage Network*, Information Warfare Monitor, 1 de septiembre de 2009, www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/. "En último término, la investigación reveló una red de más de 1 295 computadoras centrales infectadas en 103 países. Hasta un 30% de las computadoras centrales infectadas se consideran objetivos de alto valor e incluyen computadoras situadas en ministerios de asuntos exteriores, embajadas, organizaciones internacionales, medios de comunicación y ONG. Los sistemas informáticos tibetanos que investigamos manualmente, y a partir de los cuales comenzaron nuestras investigaciones, estaban gravemente afectados por numerosas infecciones que dieron a los perpetradores del ataque un acceso sin precedentes a información potencialmente delicada… pero atribuir todos los programas informáticos dañinos de origen chino a operaciones de obtención de información deliberadas o dirigidos por parte del Estado chino es falso y resulta engañoso. Las cifras pueden narrar una historia distinta. En la actualidad, China representa la mayor población mundial de Internet. El mero número de jóvenes digitales nativos en línea explica de sobra el incremento de los programas informáticos dañinos chinos. Con un mayor número de personas creativas que utilizan computadoras, se espera que China (y los chinos) representen una mayor proporción de ciberdelito."

para introducirse en las redes de las principales empresas financieras, de defensa y tecnológicas y de las instituciones de investigación de los Estados Unidos".[94]

Como demuestra el incidente de Estonia, los ciberataques intensivos y sostenidos pueden constituir en la práctica un ataque directo y sustantivo contra las entidades civiles y estatales que va más allá de la mera criminalidad. Tales ataques se caracterizan porque pueden incluir: a) graves daños físicos a instalaciones esenciales; b) lesiones o pérdidas de vidas generalizadas; c) la desestabilización de las instituciones financieras; y d) la interrupción del funcionamiento de infraestructuras esenciales. La coordinación o continuidad de tales ataques a lo largo de periodos prolongados pueden multiplicar la gravedad de las consecuencias. En tales circunstancias, con independencia de que se conozcan las identidades o los motivos del atacante, los Estados-nación pueden considerar[95] un ciberataque generalizado como un acto de terrorismo o como un equivalente funcional de un ataque armado, que justifica una consideración especial y un tratamiento específico para contrarrestarlo.

Como mínimo, la demostrada posibilidad de alteración a gran escala de una sociedad de la información exige una cultura de cooperación mutua por encima de las fronteras nacionales. En el ejemplo de Estonia, la primera oleada de alteraciones de los sitios gubernamentales puso en marcha planes de respuesta que preveían una oleada de ataques sobre servicios financieros tales como la banca en línea. De hecho, en el plazo de unos pocos días, "la banca privada y los medios en línea también fueron objetivos importantes, y los ataques afectaron al funcionamiento del resto de la infraestructura de red en Estonia".[96] Durante ese mismo periodo, las contramedidas emprendidas con la colaboración de los PSI de todo el mundo consistieron en extender el bloqueo del tráfico procedente de grupos específicos de direcciones IP y en aislar al sistema bancario de Estonia de todo el tráfico internacional. Cabe destacar que la red de recursos necesarios para hacer frente a los ciberataques superó con mucho los recursos utilizados para lanzar estos últimos.

---

94 Ariana Eunjung Cha y Ellen Nakashima, "Google China cyberattack part of vast espionage campaign, experts say", *The Washington Post*, 14 de enero de 2010, www.washingtonpost.com/wp-dyn/content/article/2010/01/13/AR2010011300359.html.

95 Por ejemplo, en 2009 el ex-Director Nacional de Inteligencia Mike McConnell calificó a las armas como armas de destrucción masiva (al menos potencialmente). Informe CRS, pág. 3.

96 "ENISA commenting on massive cyber attacks in Estonia", nota de prensa de ENISA, 24 de mayo de 2007, www.enisa.europa.eu/act/cert/contact/press-releases/enisa-commenting-on-massive-cyber-attacks-in-estonia.

La considerable asimetría entre el ataque y la defensa en el ciberespacio no ha pasado desapercibida. A falta de ataques a tan gran escala, los organismos militares y de inteligencia de los Estados Unidos y de otros Estados-nación (Rusia, China, India, Pakistán, Irán) ya están "explorando y realizando pruebas para identificar las redes digitales que pueden explotarse para aprovechar las debilidades de los posibles adversarios". Los responsables políticos de estos países actúan como si ya estuviéramos en la era del ciberconflicto. De hecho, son países como los Estados Unidos los que disponen de una capacidad asimétrica para lanzar o amparar ciberataques (especialmente como operaciones encubiertas) sobre países menos capaces de responder en consecuencia. Por otra parte, las autoridades de éstos y otros países son muy conscientes de que la importante asimetría entre el ataque y la defensa, cuando va acompañada del casi anonimato de un agresor decidido, ofrece la posibilidad de emplear, de manera directa o indirecta, pequeños "ejércitos" de cibermercenarios o "combatientes ilegales" que ofrecen a las autoridades nacionales argumentos plausibles para negar la autoría del ataque.

En la práctica, el daño potencial de un ataque concreto puede variar mucho en función del grado de preparación de la sociedad y de la seguridad integrada dentro de la estructura objeto del ataque. Desde el punto de vista del responsable político o militar, "lo importante a la hora de contrarrestar cualquier forma de ciberataque es determinar rápidamente de qué tipo de ataque se trata y quién es el adversario, y luego responder de manera apropiada. En la actualidad, la localización de las intrusiones informáticas es un cometido de las fuerzas del orden. … Las fuerzas armadas tradicionales tienen prohibido realizar esta misión en el interior del país… [en consecuencia] las fuerzas del orden cumplen un papel esencial en la seguridad y la defensa nacionales."[97] De ello se deduce que los Estados-nación requieren, tanto para sus fuerzas armadas como para sus fuerzas del orden, poderosas herramientas forenses digitales, una estructura legal apropiada para poder utilizarlas, enfoques fiables para preservar la integridad de las pruebas, y penas para los infractores que tengan un verdadero valor disuasorio. Dado que tales herramientas pueden tener un "doble uso", los países que adquieran las capacidades defensivas y forenses mayores y más flexibles dispondrán, como es lógico, de considerables capacidades de ataque y ciberespionaje. Mientras que la posibilidad de "doble uso" y la asimetría entre ataque y defensa también están presentes en el campo del armamento tradicional, la

---

97 Bonnie N. Adkins, "The Spectrum Of Cyber Conflict: From Hacking to Information Warfare: What Is Law Enforcement's Role?" Air Command and Staff College, Maxwell Air Force Base, AU/ACSC/003/2001-04, abril de 2001, http://stinet.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA406949.

probabilidad de ataques físicos se cohíbe (aunque no se elimina) mediante la disuasión y por la relativa facilidad de atribución de la autoría del ataque.

Interacción entre el conflicto tradicional y el conflicto cibernético

La fuerte penetración de las nuevas tecnologías de la información refuerza e incrementa las capacidades de combate de los armamentos convencionales y de la tecnología militar. Las tecnologías de la información hacen posibles cambios cualitativos en los campos militar, del reconocimiento y de las comunicaciones. Permiten un gran aumento de la velocidad de procesamiento de enormes cantidades de datos y la toma de decisiones operativas complejas, haciendo con ello posible la transición a métodos radicalmente nuevos de control de las tropas y del armamento en todos los planos – desde el estratégico hasta el táctico.

Las nuevas tecnologías de la información desarrollan enormemente las capacidades de combate de las instalaciones de guerra electrónica y dan lugar a nuevos tipos de armas, y más concretamente, armamento diseñado específicamente para dañar las estructuras de información civil y militar del adversario penetrando en sus redes informáticas.

Para las fuerzas armadas, la revolución informática y tecnológica permite un importante aumento de las capacidades de combate de las tropas, no sólo por cambiar las modalidades y métodos de distintas escalas de combate, sino por cambiar también el paradigma tradicional del enfrentamiento militar y de la escalada de los conflictos. Según expertos estadounidenses, dirigir armas informáticas de manera selectiva contra la infraestructura informática esencial civil y militar del adversario podría poner fin a un conflicto incluso antes de que las partes inicien operaciones de combate convencionales, dado que una escalada de ataques cibernéticos resulta catastrófica. La posesión de armamento cibernético proporciona una superioridad aplastante sobre las naciones que carecen de él. En el próximo futuro, por no decir hoy, las variables informáticas y políticas de la confrontación entre las potencias serán más importantes que las variables nucleares. Por contraste, todos los países, y en especial los más desarrollados, son vulnerables frente al armamento cibernético. El armamento cibernético, al igual que el nuclear, puede servir como un factor tanto de presión política como de disuasión.

La guerra informática no es una realidad virtual de juegos de computadora, sino una herramienta muy concreta para alcanzar la victoria en un conflicto político o militar. Sin duda alguna, el armamento cibernético se está convirtiendo en un componente principal del poderío militar de una nación, y muchos países, en particular los Estados

Unidos y China, se están preparando constante y activamente para la guerra informática.

Características del armamento cibernético

Un problema conceptual a la hora de formular un paradigma de seguridad de la información es la definición e identificación del "armamento cibernético". ¿Cuáles son las características específicas del armamento cibernético? ¿Qué nivel de ciberconflicto debería tratarse como un conflicto armado? La falta de un consenso internacional sobre estas cuestiones impide iniciar negociaciones constructivas sobre la seguridad informática mundial. Una manera de enfocar la definición del "armamento cibernético" se basa en su capacidad para afectar a la infraestructura informática militar y civil.[98] El inconveniente de este enfoque es que cualquier tipo de armamento, incluido el convencional, podría designarse como armamento cibernético si es capaz de dañar componentes de la infraestructura informática. Por ejemplo, ¿tiene importancia saber qué dispositivo ha dejado inoperante el sistema de control de una economía municipal – ya se trate de un código de programa, un impulso electrónico intenso o el impacto directo de un explosivo convencional? Otra manera de enfocar la cuestión podría ser la de considerar como armamento cibernético todos aquellos medios de destrucción que recurren a las TIC.

Al abordar la cuestión del ciberconflicto, lo que debe evitarse es rebajar el listón para la entrada en combate adoptando definiciones que incluyen actividades que se desarrollan habitualmente en tiempo de paz. ¿Cuáles son las características peculiares del armamento cibernético? ¿Qué nivel de ciberconflicto debería considerarse equivalente a un conflicto armado? Tratar como "conflicto armado" conflictos que no entrañan una amenaza clara a la vida humana o a la libertad de la sociedad resultaría imprudente y peligroso para la estabilidad internacional. Por otra parte, como la práctica totalidad de los sistemas de armamento sofisticados utilizan las TIC, resulta extremadamente difícil, por no decir imposible, aislar el armamento cibernético de toda la gama de armamento. Dado que la guerra de la información es un fenómeno constante en la historia del conflicto humano, resulta especialmente difícil encontrar

---

98 Por ejemplo, "Toda capacidad, aparato o compilación de capacidades y técnicas que, de utilizarse para la finalidad pretendida, es capaz de suponer un perjuicio para la integridad o disponibilidad de datos, un programa o la información ubicada en una computadora o en un sistema de proceso de información". Graham H. Todd, "Armed Attack In Cyberspace: Deterring Asymmetric Warfare With An Asymmetric Definition", *Air Force Law Review*, Vol. 64, 2009 págs. 65 a 102, http://lawlib.wlu.edu/CLJC/index.aspx?mainid=418&issuedate=2010-03-23&homepage=no.

una definición clara, pues se plantean varios niveles de complejidad conceptual. Por ejemplo, ¿cómo cabría clasificar la transmisión deliberada de información errónea? ¿Cómo considerar el espionaje o la intercepción de flujos de información? La perspectiva aplicable a tales actividades se vería fuertemente influida en caso de que se llevaran a cabo durante el transcurso de una guerra convencional.

Las características operativas importantes del armamento cibernético son las siguientes: 1) su costo relativamente bajo y su accesibilidad; 2) la posibilidad implícita de desarrollo, acumulación e introducción; y 3) su extraterritorialidad y la imposibilidad de atribuir la autoría de las repercusiones. Estas características hacen posible la expansión sin control del armamento cibernético y convierten su posesión por regímenes agresivos en un peligroso problema de alcance mundial. La amenaza resultante para la paz y estabilidad internacionales requiere que la comunidad mundial controle las amenazas contra la seguridad de las infraestructuras nacionales y mundiales mediante la adopción de medidas concretas orientadas a la neutralización de las ciberamenazas. En consecuencia, al integrarse en la infraestructura de una sociedad moderna, las TIC forman parte del conjunto de instrumentos de que dispone una nación para combatir a sus enemigos.

Numerosos países están adoptando medidas para contrarrestar las amenazas a la seguridad de la información; sin embargo, la eficacia de medidas incluso drásticas se ve reducida por el carácter transnacional de la amenaza y el anonimato de los trasgresores. En tales circunstancias, ninguna nación puede considerarse segura si trata de luchar contra las amenazas informáticas por sí sola. Sólo la creación de un sistema internacional de seguridad de la información y los esfuerzos concertados de sus participantes pueden paliar la proliferación del armamento cibernético y reducir las amenazas de guerra informática, terrorismo cibernético y ciberdelito.

Como mínimo, cabe considerar sin ambigüedad como armamento cibernético aquellos programas informáticos que están destinados exclusivamente a destruir la infraestructura informática (distintos virus, marcadores de páginas, etc.). La mayoría de los sofisticados medios de lucha armada que recurren a las TIC son de uso múltiple, es decir, están destinados no sólo a destruir las infraestructuras informáticas, sino también a otras tareas de combate. Las naciones que poseen estos sofisticados sistemas de armamento, medios de reconocimiento, comunicación, navegación y control basados en la aplicación a gran escala de las TIC desarrollan una ventaja militar decisiva. Y, en consecuencia, es dudoso que se lleguen a integrar alguna vez en acuerdos que limiten sus ventajas estratégicas.

Por consiguiente, es probable que la cuestión de prohibir o limitar la producción, proliferación y aplicación de armamento cibernético se limite al armamento destinado

exclusivamente a destruir elementos de la infraestructura informática, por ejemplo, el armamento basado en códigos de programa, esto es, los distintos virus y los medios para introducirlos. Por desgracia, la inmensa mayoría de las TIC modernas que pueden utilizarse con fines militares, terroristas y criminales, se desarrolla en las industrias civiles. En consecuencia, resulta muy difícil controlar su desarrollo y proliferación.

La amenaza que plantean los instrumentos para el ciberconflicto y la guerra informática es real para todos, y en especial para las naciones avanzadas, donde la complejidad de la infraestructura informática resulta determinante para todas sus actividades esenciales.[99] Solamente a través de esfuerzos concertados de la comunidad internacional para garantizar la seguridad de las infraestructuras informáticas esenciales de los países se podría reducir la amenaza de utilización maliciosa de la tecnología de la información. El consenso respecto de esta clase de sistemas informáticos permitirá una disuasión más efectiva, así como medidas de protección más eficaces, incluido el derecho a recurrir a acciones de represalia en caso de que tengan consecuencias directas graves e inaceptables. Incluso en este caso ha de ejercerse la mayor prudencia. No se justificaría iniciar una guerra convencional como consecuencia de cualquier acto cibernético agresivo; no sería prudente ofrecer a los gobiernos argumentos para decidir al respecto por sí solos.

Limitación del ciberconflicto

La enorme asimetría potencial entre las tecnologías informáticas ofensivas y defensivas hace que cualquier usuario final pueda lanzar "ciberguerras" personales contra la infraestructura informática esencial de una nación casi con la misma fuerza que los Estados-nación. Por lo tanto, el régimen político y legal para desalentar y limitar el ciberconflicto entre naciones se relacionará en la práctica con los marcos jurídicos y de procedimiento para disuadir y enfrentarse al ciberterrorismo y al ciberdelito.

En el contexto de la sociedad de la información, el concepto de disuasión a través de sanciones civiles y penales puede funcionar en el plano de la criminalidad o del

---

[99] La decisión de las fuerzas armadas de los Estados Unidos de no lanzar un ciberataque sobre los sistemas financieros iraquíes se discute en *Information Warfare and Cyberwar: Capabilities and Related Policy Issues*, Congressional Research Service, RL31787, 19 de julio de 2004, págs. 5 y 6, www.fas.org/irp/crs/RL31787.pdf. En este Informe CRS también se establece el marco militar de los Estados Unidos para la guerra electrónica y se explica el lugar que ésta ocupa dentro de la estrategia y los programas militares a largo plazo sobre guerra informática.

"hacktivismo",[100] siempre que pueda establecerse un nivel de homogeneidad internacional adaptado en los códigos penales. Lamentablemente, en el plano de los ciberataques por parte de Estados-nación, el concepto de disuasión desarrollado durante la Guerra Fría tiene escasa utilidad, ya que un contraataque similar puede dañar la conectividad social y física internacional hasta un punto que resulte inaceptable tanto para el que contraataca como para terceros. En el ciberespacio, se ha asistido en repetidas ocasiones a daños colaterales como consecuencia del rápido contagio de programas informáticos dañinos tales como los virus informáticos. En el caso intermedio del ciberterrorismo, el comportamiento reciente de los Estados Unidos respecto de los "combatientes ilegales" en su "guerra contra el terrorismo" sugiere que, también aquí, falla el modelo de disuasión a través de sanciones civiles y penales.

Aunque las dificultades de la disuasión puedan alentar la búsqueda de la defensa tecnológica perfecta contra los ciberataques, la historia de otras clases de armamento nos advierte que, en último término, lo que constituye en esencia un problema sociopolítico debe abordarse en el plano sociopolítico. En el plano político, la posible gravedad del ciberconflicto internacional requiere una atención inmediata. El doble uso característico de la tecnología obliga a descartar el tipo de régimen de control internacional utilizado para reglamentar la tecnología nuclear. Lo que sí cabe esperar (y por lo que hay que trabajar) es la creación de un marco jurídico transnacional que establezca normas y sanciones para el ciberconflicto a través de un conjunto de acuerdos estructurados, negociados en el plano internacional y vinculantes. Dichas normas deben especificar las obligaciones de las naciones signatarias respecto de las organizaciones o redes no gubernamentales encargadas del control que desarrollen sus actividades dentro de sus territorios respectivos.

Aunque en general la jurisdicción sobre los ataques de ciberterrorismo o ciberespionaje podría subsumirse en la legislación civil y penal general y en las correspondientes consideraciones en materia de jurisdicción, algunas características de los mismos podrían justificar una legislación específica que, por sí misma, diera lugar a determinadas consideraciones jurisdiccionales. Entre dichas características cabe incluir: 1) el perjuicio generalizado con connotaciones políticas; 2) una mayor dificultad para identificar, capturar y procesar a los perpetradores; y 3) la fuerte

---

[100] El Hacktivismo se refiere a elaborar o utilizar un código informático (hacking) para atacar la red de TIC señalada como objetivo con la finalidad de promover una ideología política o un objetivo social. Los hacktivistas suelen defender sus actividades como actos de protesta y desobediencia civil. A modo de ejemplo, véase http://thehacktivist.com/hacktivism.php.

presencia de una motivación política destinada a la desestabilización social, en violación de las nociones generalmente aceptadas de la legislación tanto penal como de los conflictos armados. Aún hay otro argumento a favor de un tratamiento específico del ciberterrorismo. "Una respuesta específica puede justificarse cuando el terrorismo emana de un grupo con capacidades para organizarse colectivamente de manera duradera, implicarse en planes y operaciones complejos y actuar al margen de la vida normal, o que disponga de la capacidad para intimidar a la sociedad normal a fin de que tolere su presencia".[101] El ciberconflicto prolongado entablado con fines terroristas o militares puede exigir o impulsar una acción coordinada en el plano internacional para limitar o controlar el uso de la fuerza.

Un régimen de control efectivo también debe codificar las medidas que pueden emprenderse contra atacantes no estatales siempre que, en la práctica, puedan ser identificados. En el caso de la actividad terrorista que tiene su origen en el país objeto del ataque, la acción contra el atacante puede enmarcarse en el contexto de la legislación penal existente, incluidos los estatutos contra el terrorismo. En el caso de ataques lanzados desde estados que cooperan o son neutrales, se ofrecen diversas opciones: 1) extradición al estado objeto del ataque; 2) procesamiento en el país neutral desde el que se inició el ataque; o 3) extradición a un tercer país que invoque la jurisdicción universal y disponga de unos umbrales de imperio de la ley generalmente aceptados. La opción que se escoja será cuestión de equilibrio entre la participación del estado de origen, la apariencia de justicia y el fomento de la intolerancia internacional respecto de los métodos terroristas.

El lanzamiento de ciberataques desde países carentes de escrúpulos o que no estén dispuestos a colaborar hace que sea poco probable que se recurra a los canales de cooperación normales para investigar el ataque, detener y procesar o, en su caso, extraditar a los perpetradores. La cuestión fundamental es si los atacantes serán procesados en el estado víctima de los ataques, en un tercer estado neutral o en la Corte Penal Internacional. Por consiguiente, estos casos derivan naturalmente en cuestiones de intervención por la fuerza o a través de sanciones internacionales. Estas cuestiones se asemejan a las que se plantean en casos de terrorismo por medios convencionales. Las opciones de que dispone el país víctima del ataque son:

1. represalias contra el país;

---

101 Clive Walker, "Cyber-Terrorism: Legal Principle and the Law in the United Kingdom," *Penn State Law Review,* Vol. 110, 2006, págs. 625-65, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1109113#%23.

2. la entrada sin autorización en el país y la detención de los sospechosos[102]; y
3. el debido respeto de la soberanía mediante la implicación de un tercer estado que actúe como intermediario.

Si cupiera imaginar un régimen en el que estuvieran prohibidas determinadas clases de acciones en el ciberespacio, en analogía con los Convenios de Ginebra relativos a los conflictos armados, podría pensarse en un caso de jurisdicción universal en el que interviniera un grupo internacional. Esta posibilidad lleva a entrar en el resbaladizo terreno de los argumentos respecto del desgobierno general de Internet (y su eliminación). Obsérvese que la Convención del Consejo de Europa sobre Ciberdelito no define, y por tanto no reconoce, motivos para la búsqueda transfronteriza de pruebas en las redes informáticas, incluso en caso de una persecución "en caliente".

Observaciones finales

Se reconoce lo siguiente: 1) la mayoría de las empresas, gobiernos e instalaciones de los países dependen en gran medida de las computadoras y de Internet; 2) aunque Internet es, por su propia naturaleza, resistente en lo que respecta a la conectividad, las computadoras conectadas a Internet resultan mucho más vulnerables a los ataques; 3) en la actualidad, la adquisición de capacidades de ataque poderosas requiere un nivel de inversión relativamente reducido; y 4) resulta difícil identificar con absoluta certeza la fuente de un ataque.

En lo que respecta a las leyes de la guerra, la mayoría de las naciones puede ponerse de acuerdo sobre algunos principios generales que sirvan de base para instaurar un orden armonizado en el ciberespacio.

1. Los ciberataques sobre la infraestructura esencial no son armas de ataque legítimas, ni siquiera durante los conflictos armados convencionales. (Analogía con las armas biológicas y químicas).
2. El espionaje generalizado en Internet financiado por los gobiernos hace que resulte más difícil identificar las intrusiones y perturbaciones atribuibles al crimen organizado, a las organizaciones subnacionales y a los hackers, e interfiere en el procesamiento criminal de dichos grupos en aplicación de la legislación penal en el campo de la informática.

---

102 Con arreglo a la legislación estadounidense, el hecho de llevar a un sospechoso a la jurisdicción territorial no constituye un argumento de defensa frente a la acusación.

3. El espionaje informático de baja intensidad por parte de gobiernos puede considerarse aceptable, pero se prohíbe el sabotaje. La "competencia" de baja intensidad entre los estados estimula el progreso tecnológico. Por otra parte, todo país tiene interés en saber que la seguridad de los sistemas militares extranjeros está a salvo frente a posibles delincuentes.
4. El espionaje de empresas privadas extranjeras por parte de los gobiernos tiene repercusiones difíciles de determinar, pero probablemente escasas, sobre el mundo real. No obstante, suscita un fervor nacionalista pernicioso entre los ciudadanos, envía mensajes negativos a la industria y, de hacerse a favor de la industria privada del propio país, tiende a crear un poder económico al margen de la competencia.
5. Puesto que resulta muy difícil determinar el origen de un ataque y si éste tuvo o no financiación gubernamental, las entidades no gubernamentales peligrosas pueden estar en condiciones de instigar un conflicto nacional.

Dado que podría resultar imposible verificar el cumplimiento de los acuerdos oficiales, uno de los objetivos iniciales del diálogo internacional podría ser el establecimiento de normas relativas a las pruebas necesarias para obligar al cumplimiento de las reglas del juego limpio. En este sentido, afirmaciones acerca de la ventaja económica o de la dinámica política fundamental parecen implicar una dinámica de "Guerra Fría" que socavaría los propios objetivos que tratarían de lograrse a través de un acuerdo internacional[103]. Y, lo que es más importante, de ser ciertas, ningún acuerdo de las Naciones Unidas lograría detener este proceso.

Para avanzar en la consecución del objetivo de mitigar los ciberconflictos, se requeriría una mayor reflexión teórica en los siguientes ámbitos, a fin de documentar los debates políticos que se desarrollen en instancias internacionales:

1. la teoría de la dinámica ofensiva/defensiva de la seguridad informática,
2. la dinámica ofensiva/defensiva del desarrollo de la seguridad informática en términos de beneficios de la inversión,
3. los obstáculos que unos sistemas de seguridad sólidos suponen para las operaciones (procesamiento informático, almacenamiento de datos, gestión del sistema, tiempo de la interfaz humana),

---

103 Véase el artículo "Un concepto del ciberespacio" por Henning Wegener, que figura en esta misma obra.

4. los incentivos y los elementos de disuasión para los criminales en relación con los delitos transfronterizos,
5. la repercusión del espionaje informático en los sectores público y privado.

5.2 Un llamamiento a la estabilidad geocibernética

Por Jody R. Westby

El ritmo de aumento del ciberdelito es insostenible. Los ciberdelincuentes que utilizan redes robot (*botnets*) se apropian repetidamente de datos confidenciales y patentados y llevan a cabo ataques de denegación de servicio contra sistemas de poderes públicos y empresas. Según el informe de McAfee, *2009 Unsecured Economies: Protecting Vital Information*, los encuestados perdieron en total 4 600 millones USD en materia de propiedad intelectual en 2008 y gastaron aproximadamente 600 millones USD para reparar los daños causados por violaciones de datos. Teniendo en cuenta estas cifras, McAfee estimó que, en todo el mundo, las empresas perdieron más de 1 billón USD en 2008. Los particulares deben hacer frente a la carga que representa la actualización permanente del software y los programas antivirus, pese a lo cual muchos de sus sistemas son infectados y utilizados en los ciberataques.

Los países han admitido el valor de los sistemas de sus poderes públicos y empresas, y reconocen que su seguridad económica y nacional está en peligro. Por este motivo, han comenzado a elaborar estrategias de guerra informática y a establecer cibercomandos con capacidades ofensivas y defensivas. Si bien estas acciones son apropiadas y previsibles, es notable el vacío que existe con respecto al diálogo relativo a la paz en el ciberespacio, e incluso aún más al mantenimiento de un nivel aceptable de estabilidad geocibernética. Como se indica en la Introducción, el autor define como "geocibernética" la relación entre Internet y la geografía, la demografía, la economía y la política de una nación y su política exterior. La "estabilidad geocibernética" se define como la capacidad de todos los países de utilizar Internet para su beneficio económico, político y demográfico, absteniéndose al mismo tiempo de cualquier actividad que pudiera causar un sufrimiento y una destrucción innecesarios.[104]

En parte, la reticencia de los países a participar en discusiones sobre la necesidad de contar con "comunicaciones esenciales mínimas" para preservar las funciones vitales de la sociedad y evitar el sufrimiento y la destrucción innecesarios causados por los ciberataques, puede tener su origen en una cierta incertidumbre general con respecto a la manera en que podría abordarse ese asunto en el marco jurídico internacional actual.

---

104 Presentado por primera vez en el ANSER Institute of Homeland Security Conference, "Homeland Security 2005: Charting the Path Ahead", Universidad de Maryland, Presentación de Jody Westby, "A Shift in Geo-Cyber Stability and Security", 6-7 de mayo de 2002.

Legislación en materia de conflictos armados

En el curso de la historia moderna, la legislación internacional en materia de conflictos armados (LOAC, *laws of armed conflict*) se ha actualizado en respuesta a las atrocidades de la guerra y a los nuevos métodos de lucha contra la guerra. Resulta urgente volver a hacerlo para adaptarla a las capacidades cibernéticas puesto que es probable que las acciones de la guerra cibernética violen numerosas disposiciones de la legislación vigente o no correspondan al ámbito de aplicación del conjunto de las leyes.

Los marcos jurídicos básicos que rigen los conflictos armados son muy amplios y en gran medida se han elaborado durante el siglo pasado. Entre los documentos esenciales de interés para el ciberconflicto, pueden mencionarse los siguientes:

- Carta de las Naciones Unidas[105]
- Tratado de la Organización del Atlántico Norte (OTAN)[106]
- Convenios de Ginebra de 1949[107]
- Protocolo adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la Protección de las víctimas de los conflictos armados internacionales (Protocolo I)[108]
- Convención de La Haya (1899 y 1907)[109]
- Convenio sobre Prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales que Puedan Considerarse Excesivamente Nocivas o de Efectos Indiscriminados.[110]

---

105 Carta de las Naciones Unidas, www.un.org/en/documents/charter/index.shtml.

106 Tratado del Atlántico Norte, www.nato.int/cps/en/natolive/official_texts_17120.htm.

107 Convenios de Ginebra de 1949, www.icrc.org/web/eng/siteeng0.nsf/html/genevaconventions.

108 Protocolo adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la Protección de las víctimas de los conflictos armados internacionales (Protocolo I), 8 de junio de 1977, www.icrc.org/ihl.nsf/7c4d08d9b287a42141256739003e636b/f6c8b9fee14a77fdc125641e0052b079 ("en lo sucesivo, Protocolo I").

109 Convención sobre las Leyes y Costumbres de la Guerra Terrestre (La Haya II), 29 de julio de 1899, http://avalon.law.yale.edu/19th_century/hague02.asp; Leyes y Costumbres de la Guerra Terrestre (La Haya IV), 18 de octubre de 1907, http://avalon.law.yale.edu/20th_century/hague04.asp.

Las premisas básicas de estos documentos se pueden simplificar. La legislación en materia de conflictos armados regula el curso de las hostilidades armadas, y los militares deben planificar y realizar sus operaciones en el marco de esas leyes. Se aplica a las operaciones militares y actividades afines, y su finalidad es evitar el sufrimiento y la destrucción innecesarios en la guerra. Una serie de disposiciones especiales protege a los civiles, los prisioneros, los heridos, los enfermos y los náufragos.

Realización de acciones militares

Son tres los principios básicos que rigen la *manera* en que pueden llevarse a cabo las acciones militares: necesidad, distinción y proporcionalidad.

Necesidad: Este principio indica que las fuerzas de combate deben llevar a cabo únicamente las acciones necesarias para alcanzar objetivos militares legítimos. Los equipos, instalaciones y fuerzas militares pueden constituir un objetivo si se obtiene la rendición completa o parcial del enemigo.

Distinción: Este principio exige a los militares que distingan entre objetivos lícitos e ilícitos como, por ejemplo, civiles, propiedad civil y heridos. En la medida de lo posible, los objetivos civiles deben estar separados de los objetivos militares. Se consideran ataques indiscriminados los que afectan tanto a civiles como a objetivos militares y civiles.

Proporcionalidad: Con arreglo a este principio, se prohíbe el despliegue de una fuerza superior a la necesaria para lograr objetivos militares. Este principio compara la ventaja militar alcanzada por el ataque con los daños causados y requiere un equilibrio entre la ventaja militar directa esperada y el perjuicio o daño civil previsto.

Intervención en un conflicto armado

En un conflicto armado pueden intervenir únicamente *combatientes legítimos*, es decir, personas autorizadas por los poderes públicos a participar en las hostilidades. Pueden constituir una fuerza irregular pero deben estar a las órdenes de una persona responsable de sus subordinados, exhibir signos distintivos y reconocibles a distancia

---

110 Convenio sobre Prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales que Puedan Considerarse Excesivamente Nocivas o de Efectos Indiscriminados, 28 de noviembre de 2003, www.icrc.org/web/eng/siteeng0.nsf/html/p0811 (en lo sucesivo, "Convenio sobre Armas Excesivamente Nocivas").

(como, por ejemplo, un uniforme o un determinado color), llevar sus armas a la vista y realizar operaciones con arreglo a la legislación en materia de conflictos armados.

Combatientes ilegítimos son quienes participan directamente en las hostilidades sin autorización de un poder público o sin respetar el derecho internacional. A título de ejemplo, son combatientes ilegítimos los civiles que atacan a las fuerzas armadas, los piratas y los terroristas.

Los *no combatientes* son personas no autorizadas por un poder público a participar en las hostilidades, pero intervienen en ellas. Este grupo incluye a personas tales como capellanes, civiles que acompañan a los militares y personal médico. Aunque tal vez no sean el objetivo de un ataque directo, pueden morir a consecuencia de él. Cuando se desconoce la situación de un combatiente, se aplican los Convenios de Ginebra hasta que se determine su situación.

Objetivos

Los *objetivos militares*, por su naturaleza, ubicación, finalidad o utilización, facilitan realmente la capacidad bélica de un enemigo, cuya destrucción o neutralización parcial o total en el momento del ataque favorece objetivos militares legítimos.

Los *objetivos protegidos* son estipulados por los Convenios de Ginebra; entre ellos, hospitales, transporte de enfermos o heridos, sitios religiosos o culturales y zonas de seguridad. Sin embargo, si alguno de esos objetivos se utiliza para fines militares, puede ser atacado. A título de ejemplo, cuando un militar establece su base de operaciones en una iglesia, ésta pasa a ser un objetivo militar legítimo.[111]

En el contexto cibernético, estos principios plantean algunas preguntas que aún no tienen respuesta:

- ¿Qué acción constituye un acto de ciberconflicto armado?
- Las infraestructuras básicas, ¿pueden constituir un objetivo?
- Si la infraestructura básica respalda los objetivos protegidos por los Convenios de Ginebra, ¿pueden esas redes constituir un objetivo?
- Los ataques a la infraestructura básica, ¿son necesarios para alcanzar objetivos militares?

---

111 Ver Thomas C. Wingfield, *The Law of Information Conflict: National Security Law in Cyberspace*, Aegis Research Corp., Falls Church, VA, 2000; *The Law of Armed Conflict: Basic Knowledge*, Comité Internacional de la Cruz Roja, junio de 2002, www.icrc.org.

- ¿De qué manera los participantes en las hostilidades pueden distinguir entre objetivos militares y objetivos protegidos?
- ¿El daño causado a la infraestructura básica es proporcional al causado a los objetivos militares?
- ¿Qué se entiende por fuerza excesiva en el ciberespacio?
- ¿Cómo se distinguen los cibersoldados?
- ¿Cómo se determina si un tercero actúa en nombre de un Estado-nación?

No hay ninguna respuesta clara a estas preguntas en la legislación vigente. Por ejemplo, ¿constituyen las redes de comunicaciones del sector privado en los EE.UU. un objetivo militar legítimo en el marco de la necesidad militar porque el 90 por ciento de las comunicaciones de las autoridades gubernamentales del país utilizan las redes comerciales, incluidas Internet, la telefonía, los sistemas celulares y el satélite?[112] Es indudable que las empresas y los accionistas titulares de esas redes formularán argumentos en contra de este razonamiento. Como también lo harán los hospitales, cuyas actividades dependen íntegramente de esas redes; probablemente considerarían que un ataque de ese tipo va dirigido contra un objetivo protegido.

Si la LOAC autoriza la utilización de fuerzas irregulares, ¿podrán las autoridades gubernamentales contratar piratas informáticos (*botmasters*) y utilizar sus redes robot como combatientes legítimos en los ciberconflictos? Se puede autorizar la participación de fuerzas irregulares en las hostilidades, pero las redes robot no son reconocibles ni sus armas visibles. En efecto, los robots en una red no tienen emblema ni una marca que los distinga, e incluso pueden no dejar rastro puesto que difunden sus programas malintencionados a través de páginas web, redes entre homólogos, enlaces maliciosos, sitios de redes sociales y correo basura. Una computadora personal que funciona como un robot en un ataque iniciado a instancias de un Estado-nación puede pertenecer a un civil inocente que no tiene conocimiento de que su computadora ha sido interferida. Si se detecta esa intrusión, ¿puede considerarse a ese pirata un criminal de guerra? ¿Qué se hace con los propietarios de las computadoras?

Las Convenciones de La Haya V y XIII estipulan los derechos y obligaciones de los países neutrales con respecto a la guerra terrestre y marítima, pero nada dicen con

---

112 *The Insider Threat to U.S. Government Information Systems*, National Security Telecommunications and Information Systems Security Committee, NSTISSAM INFOSEC/1-99, www.cnss.gov/Assets/pdf/nstissam_infosec_1-99.pdf.

respecto al ciberespacio. Es posible que un país no movilice tropas ni convoyes en el territorio de una nación neutral ni cometa ningún acto de hostilidad en las aguas territoriales de un país neutral, pero ¿qué ocurre si se introduce en las redes de países neutrales? ¿Deben los países pedir autorización a los países neutrales para lanzar un ciberataque a través de sus redes? Con la conmutación de paquetes, ¿cómo sabe siquiera un país qué redes se utilizarán? ¿Puede un país utilizar una red robot como fuerza irregular si ello supone la utilización de computadoras en un país neutral?

La Carta de las Naciones Unidas, el Convenio de Ginebra, la Convención de La Haya y el Tratado de la Organización del Atlántico Norte (OTAN) no se ajustan a los conflictos cibernéticos. La Carta de las Naciones Unidas y el Tratado de la Organización del Atlántico Norte (OTAN) utilizan ciertas expresiones (como, por ejemplo, "integridad territorial", "utilización de la fuerza armada", "acción de las fuerzas aéreas, terrestres o marítimas" y "ataque armado") que resultan inadecuados en el contexto cibernético, el cual, al parecer, queda fuera del ámbito de aplicación del derecho internacional. Los conflictos de Estonia y Georgia muestran de manera espectacular las consecuencias del ciberconflicto y la confusión en torno al intento de dar una respuesta, causada por la incertidumbre sobre el ordenamiento jurídico.[113]

Defensa de la estabilidad geocibernética

Lo indicado anteriormente explica sólo unas pocas incertidumbres jurídicas con respecto al ciberconflicto. Una revisión efectuada a la LOAC revela la voluntad histórica de actualizar esos documentos para que admitan nuevas tecnologías como,

---

113 Para un debate más exhaustivo sobre los conflictos de Estonia y Georgia, así como sobre las cuestiones jurídicas y vinculadas a dar una respuesta a los mismos, ver Jody R. Westby, "The Path to Cyber Stability", "*Rights and Responsibiliites in Cyberspace: Balancing the Need for Security and Liberty*", EastWest Institute and World Federation of Scientists, 2010, www.ewi.info/rights-and-responsiblities-cyberspace-balancing-need-security-and-liberty.

por ejemplo, armamento naval y aeronaves.[114] De esta forma, se podrían introducir enmiendas a esos mismos instrumentos para adaptarlos al ciberconflicto.

No obstante, la primera cuestión esencial es determinar qué grado de actividad debe ser autorizado. El autor sostiene que, en situación de ciberconflicto, deben aplicarse cuatro principios:

1. *Se debe proteger una determinada cantidad de infraestructuras básicas para evitar destrucciones, daños y sufrimientos innecesarios y garantizar un grado mínimo de comunicaciones esenciales.*

   Entre las infraestructuras básicas protegidas se incluirán las que prestan apoyo, por ejemplo, a hospitales y centros médicos, centros de asistencia, sistemas financieros, sistemas de soporte vital y dispositivos médicos fundamentales, cadenas de suministro, transporte, transmisión de noticias, instituciones educativas, iglesias y centros religiosos, servicios de auxilio y fuerzas del orden. Esta lista, que no pretende ser exhaustiva, ofrece en cambio algunos ejemplos de los tipos de sistemas que protegen a civiles inocentes, en particular a niños, enfermos y heridos, y personas de edad. Las partes interesadas deben ayudar a los diplomáticos a definir los límites sagrados de la infraestructura básica.

   Justificación: La LOAC vigente respalda este concepto, tal como se indica en las *Reglas básicas de los Convenios de Ginebra y sus Protocolos adicionales:*

   > En todo conflicto, el derecho de las Partes que intervienen en él de optar por métodos o medios de guerra no es ilimitado. De este principio se derivan dos reglas básicas. En primer lugar, se prohíbe la utilización de armas, proyectiles y materiales y métodos de guerra de tal índole que cause daños innecesarios. En segundo lugar, con objeto de garantizar el respeto y la protección de las poblaciones civiles y de la propiedad civil, las Partes en el conflicto están

---

114 Ver, por ejemplo, "Protection of civilian persons and populations in time of war", (Protección de personas y poblaciones civiles en tiempo de guerra) extraído de "Reglas básicas de los Convenios de Ginebra y sus Protocolos adicionales", Comité Internacional de la Cruz Roja, 31 de diciembre de 1988, www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV (en lo sucesivo, "Protección de personas civiles") (debido al aumento espectacular de la guerra aérea fue necesario elaborar y especificar aún más la legislación vigente en materia de conflictos armados. De este aspecto se ocupa la Parte IV del Primer Protocolo adicional de los Convenios.); se añadió el Convenio II de Ginebra con objeto de tener en cuenta la utilización de barcos de guerra y abordar el trato dispensado a los heridos, los enfermos y los náufragos de las fuerzas armadas en el mar.

> obligadas a distinguir en todo momento entre población civil y combatientes, así como entre propiedad civil y objetivos militares, y a llevar a cabo sus operaciones únicamente contra objetivos militares.[115]

Los daños y perjuicios que pudieran derivarse de la destrucción o inhabilitación de los sistemas de infraestructuras básicas son innecesarios y podrían causar privaciones y sufrimientos extremos de la índole que la legislación en materia de conflictos armados trata de impedir. Por otra parte, dado que esas redes prestan servicio a grandes poblaciones, los daños y perjuicios causados por ese tipo de ataque se propagarían y no serían proporcionales a la ventaja militar.

Numerosas disposiciones del Convenio IV de Ginebra respaldan este principio propuesto. El Convenio se refiere específicamente a la protección de personas civiles y, en particular, protege a los heridos, los enfermos, los inválidos y las mujeres encinta (Art. 16). Durante las hostilidades, toda parte podrá proponer zonas neutralizadas en las regiones en conflicto para proteger a los heridos y enfermos, combatientes o no combatientes, así como a las personas civiles que residen en dichas zonas pero no participan en las hostilidades ni realizan trabajo alguno de índole militar (Art. 15). En ninguna circunstancia, podrán ser objeto de ataques los hospitales civiles organizados para prestar asistencia a los heridos, a los enfermos, a los inválidos y a las parturientas (Art. 18). Se debe procurar a los niños menores de quince años que hayan quedado huérfanos o que estén separados de su familia a causa de la guerra la manutención, la práctica de su religión y la educación (Art. 24). Está prohibida la destrucción de bienes muebles o inmuebles, pertenecientes individual o colectivamente a personas particulares, al Estado o a colectividades públicas, a organizaciones sociales o a cooperativas (Art. 53).

El Protocolo I del Convenio de Ginebra es un texto complementario del Convenio IV y amplía el alcance de la protección de personas civiles en tiempo de guerra. Los Artículos 48 a 59 del Protocolo I son particularmente importantes. Una persona civil es toda aquella que no forma parte de las fuerzas armadas (Art. 50). Las personas civiles gozarán de protección general contra los peligros procedentes de operaciones militares, no serán objeto de

---

115 "Protection of civilian persons and populations in time of war", extraído de "Reglas básicas de los Convenios de Ginebra y sus Protocolos adicionales", Comité Internacional de la Cruz Roja, 31 de diciembre de 1988, www.icrc.org/web/eng/siteeng0.nsf/html/57JMJV.

ataque ni de actos cuya finalidad principal sea aterrorizar a la población civil, o de ataques indiscriminados que no estén dirigidos contra un objetivo militar concreto (se consideran indiscriminados los ataques que pudieran causar incidentalmente muertos y heridos entre la población civil, o daños a bienes de carácter civil, que serían excesivos en relación con el objetivo militar) (Art. 51). Los bienes de carácter civil no serán objeto de ataques ni de represalias; en caso de duda, se dará por supuesto que se trata de un bien de carácter civil (Art. 52). Queda prohibido cometer actos de hostilidad dirigidos contra monumentos históricos, obras de arte o lugares de culto (Art. 53). Quedan prohibidos los ataques a bienes indispensables para la supervivencia de la población civil (tales como artículos alimenticios y las zonas agrícolas que los producen, las cosechas, el ganado, las instalaciones y reservas de agua potable y las obras de riego) (Art. 54). No serán objeto de ataques las obras o instalaciones que contienen fuerzas peligrosas, a saber, las presas, los diques y las centrales nucleares, aunque sean objetivos militares legítimos, cuando tales ataques puedan producir la liberación de aquellas fuerzas y causar, en consecuencia, pérdidas importantes en la población civil (Art. 56). Se llevará a cabo un cuidado constante para preservar a la población civil (Art. 57). Quienes preparen un ataque deberán hacer todo lo que sea factible para verificar que los objetivos que se proyecta atacar no son personas civiles ni bienes de carácter civil, ni gozan de protección especial, y tomarán todas las precauciones posibles para evitar o, como mínimo, reducir el número de muertos y de heridos que pudieran causar incidentalmente entre la población civil (Art. 57). Queda prohibido atacar localidades no defendidas (no hay operaciones militares ni personal en la zona) (Art. 59).

Además, la LOAC contiene numerosas disposiciones, añadidas en los últimos años, que prohíben la utilización de tecnologías que son excesivamente nocivas o que podrían tener efectos indiscriminados. Ya en 1899, en la Convención de La Haya se adoptaron una serie de declaraciones destinadas a prohibir el lanzamiento de proyectiles y explosivos desde globos "o por otros nuevos métodos de naturaleza similar"[116], la utilización de proyectiles que difunden gases asfixiantes o deletéreos[117] y la utilización de balas expansivas

---

116 Declaración sobre la prohibición del lanzamiento de proyectiles y explosivos desde globos (La Haya, IV); 29 de julio de 1899, http://avalon.law.yale.edu/19th_century/hague994.asp.

117 Declaración sobre la utilización de proyectiles que suponen la difusión de gases asfixiantes o deletéreos, Conferencia de La Haya, 29 de julio de 1899, http://avalon.law.yale.edu/19th_century/dec99-02.asp.

o de aplastamiento.[118] En 2001, se adoptó la Convención sobre prohibiciones o restricciones del empleo de ciertas armas convencionales que puedan considerarse excesivamente nocivas o de efectos indiscriminados, en virtud de la cual se prohíbe una amplia gama de armas particularmente peligrosas y nocivas, incluidas aquellas cuya mención se remonta a 1899, así como minas terrestres, armas trampa, armas incendiarias, armas láser que producen ceguera y restos explosivos de guerra.[119] Esta Convención podría ser objeto de una enmienda para contemplar los ciberataques contra infraestructuras básicas definidas.

2. *Se debe proscribir la utilización de redes robot y otras ciberfuerzas irregulares.*

   Justificación: Cuando comienza un ataque, la víctima no puede hacer una distinción entre esos combatientes y cualquier otro atacante; no sabe si la persona que ataca su sistema tiene acceso a información confidencial (*insider*) o si es un pirata informático solitario, un ciberdelincuente, un criminal organizado y de gran capacitación, un terrorista o un Estado-nación. Resulta difícil seguir el rastro de las actividades vinculadas al ciberdelito y a veces no se puede determinar quién es el responsable, aunque investigadores expertos se ocupen de examinar el caso. Además, es imposible distinguir un cibersoldado puesto que no exhibe ningún signo distintivo y, efectivamente, no se distingue a distancia. Por este motivo, las ciberfuerzas irregulares violan una de las reglas básicas del conflicto armado.

3. *Los países deben respetar la neutralidad de otros países y no transmitir ningún tipo de ataque a través de sus infraestructuras básicas. (Convenciones V y XIII de La Haya).*

   Este principio está en armonía con las Convenciones de La Haya que restringen el transporte de tropas o convoyes de suministros y municiones a través de territorios o aguas neutrales. Muchas infraestructuras básicas como, por ejemplo, las redes eléctricas, pueden ser destruidas por sobrecargas en el sistema. Por lo tanto, autorizar a los países a llevar a cabo ciberataques que supongan el tránsito por redes de otras naciones sin su conocimiento es sencillamente incompatible con la historia y la finalidad de la LOAC. Mediante este principio propuesto, se exigirá a los países obtener el

---

118 Declaración sobre la prohibición del uso de balas que se expanden o aplastan fácilmente en el cuerpo humano, Conferencia de La Haya, 29 de julio de 1899, http://avalon.law.yale.edu/19th_century/dec99-03.asp.

119 Convenio sobre armas excesivamente nocivas.

permiso de otros países antes de lanzar un ciberataque, con lo cual servirá como elemento disuasivo de los ciberconflictos.

4. *Los países deben ayudarse mutuamente en sus investigaciones sobre actividades vinculadas al ciberdelito.*

   Con objeto de garantizar un cierto grado de estabilidad geocibernética, es esencial la cooperación de los proveedores de servicios Internet (PSI) y de otras autoridades gubernamentales en la investigación de actividades vinculadas al ciberdelito. Aunque pueda parecer contradictorio exigir a un país neutral que colabore en una investigación, incluso en tiempo de guerra, todos los ciberataques son inicialmente similares. Será únicamente gracias a la investigación que la víctima podrá hacerse una idea de quién podría ser el atacante. Como principio básico, los países que deseen estar conectados a Internet tienen la obligación de garantizar que tanto ellos como los proveedores presentes dentro de sus fronteras prestan ayuda en las investigaciones sobre ciberdelitos. Si se autorizara a los países a rechazar ese tipo de asistencia en nombre de la neutralidad, todos los ciberdelincuentes dispondrían del tiempo necesario para saquear los países que participan en las hostilidades. En sentido inverso, si se negaran a prestar esa asistencia, los países neutrales podrían en realidad ayudar o incluso incitar a los delincuentes o al país atacante. En el contexto del ciberataque, sólo a través de la asistencia un país podrá seguir siendo verdaderamente neutral.

Hacer realidad la estabilidad geocibernética

Internet ha creado un ciberplaneta que no reconoce las fronteras tradicionales y actúa en gran medida al margen del control gubernamental. Constituye una nueva forma de armamento que presenta un riesgo sin precedentes para los civiles, especialmente los niños, las personas de edad, los enfermos y las personas frágiles o con discapacidad. Además, modifica completamente la legislación en materia de conflictos armados puesto que, en un ciberconflicto, es más probable que los objetivos sean de carácter civil y no militar y que afecten más a la población civil que a las tropas militares. En la mayoría de los países, las infraestructuras básicas pertenecen al sector privado, que se encarga de explotarlas. Por lo tanto, los ataques a la infraestructura básica se equiparan a los ataques contra la población civil y las redes que sustentan su vida y sus medios de subsistencia. No puede ignorarse la necesidad urgente de actualizar la legislación en materia de conflictos armados para tener en cuenta esta nueva amenaza dado que es muy fácil interpretar la *falta* de un marco jurídico como aprobación de los ataques desde el punto de vista jurídico.

Algunos expertos jurídicos y en seguridad reclaman una ley o un tratado de envergadura sobre el ciberespacio. Sería absurdo. En el curso de la evolución de fuerzas navales, flotas aéreas y otras tecnologías, la LOAC ha sido adaptada conservando un marco legislativo coherente pero en evolución. Además, hay consideraciones de carácter pragmático. Los tratados plantean problemas y, en su etapa de redacción, requieren prolongadas discusiones multilaterales seguidas de un proceso de apertura a la firma. A continuación, los signatarios deben ratificar el tratado y aplicarlo en la legislación nacional. Por lo general, un cierto número de signatarios debe ratificar el tratado antes de su entrada en vigor, e incluso entonces sólo cobra efectividad para los países que lo han ratificado y aplicado. Este procedimiento lleva tiempo, lo que redundará en ventaja de los ciberdelincuentes o personas malintencionadas.

En cambio, los instrumentos en vigor, como la Carta de las Naciones Unidas, el Tratado de la Organización del Atlántico Norte (OTAN), el Convenio de Ginebra y la Convención de La Haya pueden ser modificados *y* tienen la ventaja de que ya han sido ratificados y aplicados en la legislación nacional.

En el ciberespacio, donde los minutos cuentan, la solución obvia es la más expeditiva. Los Estados nacionales deben aunarse, con el aporte brindado por los interesados, para formular las siguientes modificaciones en la actual legislación internacional en materia de conflictos armados:

1. La Carta de las Naciones Unidas debe ser modificada para tener en cuenta los ciberconflictos y aclarar que la "integridad territorial" incluye las infraestructuras básicas y la disponibilidad, integridad y confidencialidad en la esfera cibernética. En concreto, debe modificarse el Artículo 42 para que el Consejo de Seguridad pueda llevar a cabo su acción por medios cibernéticos.
2. La Carta de la OTAN, debe ser modificada para autorizar la defensa colectiva en virtud del Artículo 5. La expresión "ataque armado" contemplada en el Artículo 6(1) no debe limitarse a "territorios" ni a "fuerzas, buques y aeronaves" y deberá abarcar los ciberataques.
3. Las Convenciones de La Haya deben ser modificadas para proscribir la utilización de fuerzas irregulares en el cibercombate y prohibir la transmisión de ciberataques a través de las redes de países neutrales.
4. Los Convenios de Ginebra deben ser modificados para proscribir los ataques a infraestructuras básicas que pudieran dañar comunicaciones esenciales mínimas y poner en peligro a poblaciones civiles.

A este respecto se necesita un nuevo acuerdo. Separadamente, los países deben ponerse de acuerdo para cooperar y contribuir a la investigación de actividades

vinculadas al ciberdelito cuyo tránsito, según estiman, ha pasado por sus redes. Los países no signatarios de ese acuerdo no podrán interponer recursos ante la legislación internacional si otras naciones bloquean las comunicaciones de su país.

Las consideraciones precedentes servirán para que los Estados-nación y los particulares tengan confianza en las TIC y sigan integrándolas en su vida y sus sociedades sin miedo a que se conviertan en blanco de un ciberconflicto. De esta forma se iniciará también un diálogo constructivo entre los países, en el cual, por primera vez, todos encarnarán una posición común.

6 Ciberespacio

Un concepto de ciberespacio

Por Henning Wegener

Este libro trata de la paz en el ciberespacio (o ciberpaz) y se distingue claramente de los fenómenos negativos de la guerra en el ciberespacio (o ciberguerra), el ciberterrorismo y el ciberdelito. Optar por el aspecto positivo de la antinomia guerra-paz implica un cambio importante en la perspectiva y el establecimiento de prioridades dado que apunta a las ventajas y posibilidades positivas de la sociedad de la información y proporciona una finalidad en ese sentido, refuerza la connotación negativa de la ciberguerra así como de la terminología y calamidades que genera, e impulsa la cultura mundial de la ciberseguridad.

En este intento de deslegitimar la ciberguerra cambiando de perspectiva se tiene plenamente en cuenta la omnipresencia actual de las infraestructuras digitales que, inevitablemente, también serán utilizadas para fines hostiles y no pacíficos. El objetivo primordial es pues encauzar esas utilizaciones y determinar los límites más estrictos posibles para cualquier aplicación beligerante de las TIC. Dado que la propia expresión "ciberguerra" es propicia para estimular esquemas de mentalidad militar y concebir la ciberdefensa básicamente desde el punto de vista de la acción y las técnicas militares ("represalia"), en este capítulo se tratará de combatir este automatismo mental y corroborar la defensa de un comportamiento pacífico en el ciberespacio. Sin embargo, no será más que el esbozo de un respaldo conceptual a la ciberpaz, que será necesario desarrollar con el transcurso del tiempo. Muchas otras secciones de este libro contribuyen a esta tarea.

Durante varios años, incluso en reuniones públicas y publicaciones, la Federación Mundial de Científicos situó el concepto de paz en el ciberespacio en el centro de su labor[120], y la UIT, en particular a través de su Secretario General, ha contribuido

---

120 Ver diversas referencias consultando "publicaciones" y "actividades" en www.unibw.de/infosecur, entre las últimas concretamente la transcripción de una conferencia celebrada en diciembre de 2008, con el nombre de "The Global Internet Crisis: The Quest for Cyber Peace" (La crisis mundial de Internet: la búsqueda de la paz en el ciberespacio).

recientemente a darle un carácter más concreto.[121] Pero, evidentemente, este concepto ha sido utilizado con anterioridad, si bien no en forma tan exhaustiva. La utilización más notable del término, aunque específica y limitada, y en este caso referida a los niños, fue llevada a cabo por Egipto en 2007 durante la promoción del programa Iniciativa sobre ciberpaz, en el marco del Movimiento Internacional de Mujeres en pro de la Paz Suzanne Mubarak (SMWIPM)[122], que hace referencia directa a la Declaración y Programa de Acción sobre una Cultura de Paz, de las Naciones Unidas. La misión de la Iniciativa es facultar a los jóvenes de todo el mundo a través de la creación de capacidades TIC, la seguridad de Internet y el fomento de la innovación. El término ciberpaz también está presente ocasionalmente, aunque en forma no sistemática e indefinida, en las actividades de la comunidad de investigaciones sobre la paz.

En el contexto actual, se considera que la ciberpaz, entendida en un sentido más amplio que el formulado en el SMWIPM, constituye un principio primordial en el establecimiento de un "orden universal del ciberespacio". Si su aplicación está más vinculada a aspectos o prioridades de carácter político y a una reflexión sobre las verdaderas opciones, este término debe por tanto, en cierta manera, seguir siendo indefinido. La definición no puede ser hermética sino más bien intuitiva y gradual teniendo en cuenta sus numerosos elementos.

Con todo, se necesita una definición básica. El punto de partida para cualquier intento de definición debe ser el concepto general de la paz, es decir, una situación de tranquilidad saludable, la ausencia de desorden o perturbaciones y violencia, la ausencia no sólo de la utilización de la fuerza o violencia "directa" sino también de restricciones indirectas. La paz implica el predominio de principios, posibilidades y procedimientos morales generales para la solución de conflictos, la durabilidad y la estabilidad.

Debemos a la Asamblea General de las Naciones Unidas su gran intento de formular el concepto de paz, y de una cultura de paz, otorgándole un contenido de importancia fundamental. Su "Declaración y Programa de Acción sobre una Cultura de Paz " de

---

121 "El Secretario General de las Naciones Unidas propuso un acuerdo internacional para evitar la guerra en el ciberespacio", 31 de enero de 2010, www.thepoc.net/breaking-news/world/3930-un-chief-proposes-intl-a.

122 Movimiento Internacional de Mujeres en pro de la Paz Suzanne Mubarak, Iniciativa sobre ciberpaz, http://smwipm.cyber peaceinitiative.org/.

octubre de 1999[123] establece un catálogo de componentes y condiciones previas de la paz, y define la manera de alcanzarla y mantenerla a través de una cultura de paz. Recordando la Constitución de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, en la cual se establece que "puesto que las guerras nacen en la mente de los hombres, es en la mente de los hombres donde deben erigirse los baluartes de la paz", la Resolución describe los elementos de forma exhaustiva y establece su programa de acción para el decenio (hasta 2010).

Los fundamentos importantes de la paz y de una cultura de paz no se limitan a la no utilización de la fuerza, y a la promoción y práctica de la no violencia; suponen además una serie compartida de valores y estilos de comportamiento, el orden y la legalidad internacional, procesos de participación positiva y los derechos humanos (se cita, entre otras cosas, la adhesión a los principios de libertad, justicia, democracia, tolerancia, solidaridad, cooperación, pluralismo, diversidad cultural, diálogo y entendimiento, así como la promoción de la solución de conflictos). Aparte del gran hincapié que debe hacerse en los componentes éticos de la paz, en un contexto cibernético resulta particularmente importante que en ese catálogo se contemplen, entre los requisitos previos de la paz, el respeto y fomento del derecho de todos a la libertad de expresión, de opinión y de información, así como el acceso a la información. Naturalmente, estas referencias son únicamente a título indicativo; la Resolución, en su conjunto, merece un examen detenido. Recientemente, la UIT ha formulado cinco principios sobre la ciberpaz que también establecen acciones y obligaciones concretas que garantizarán la paz y la estabilidad en el ciberespacio. Se remite al lector a esta lista dada su importancia esencial.

La Federación Mundial de Científicos, por su parte, se ha encargado de traducir los principios generales que allí figuran, así como otros principios generales aprobados por las Naciones Unidas aplicables al entorno cibernético de manera un poco más detallada, en su "Declaración Erice de Principios sobre la ciberestabilidad y el ciberespacio" de agosto de 2009.[124] Esa Declaración muestra la estrecha vinculación entre el logro de la ciberestabilidad y de la ciberpaz. La Declaración es concisa y se concentra en los elementos esenciales de funcionamiento del ciberespacio, enumerados a continuación:

---

123 "Declaración sobre una Cultura de Paz", UNESCO, A/Res/53/243, www.unesco.org/cpp/uk/declarations/2000.htm.

124 "Declaración Erice de Principios sobre la ciberestabilidad y el ciberespacio", Federación Mundial de Científicos, agosto de 2009, www.ewi.info/system/files/**Erice**.pdf.

1. Todos los gobiernos deben reconocer que el derecho internacional garantiza a las personas el libre flujo de información e ideas; esas garantías también se aplican al ciberespacio. Se tendrán únicamente en cuenta las restricciones necesarias y acompañadas de un procedimiento de revisión jurídico.
2. Todos los países deben trabajar juntos para elaborar un código común de ciberconducta y un marco jurídico mundial armonizado, incluidas disposiciones de procedimiento relativas a la asistencia y cooperación en materia de investigación que respete la privacidad y los derechos humanos. Todos los gobiernos, proveedores de servicios y usuarios deben respaldar el cumplimiento del derecho internacional contra los ciberdelincuentes.
3. Todos los usuarios, proveedores de servicios y autoridades gubernamentales deben tratar de garantizar que el ciberespacio no se utilice de modo que dé lugar a la explotación de los usuarios, en particular los jóvenes y personas indefensas, a través de la violencia o la degradación.
4. Las autoridades gubernamentales, las organizaciones y el sector privado, incluidos los particulares, deben llevar a cabo y mantener programas de seguridad integral basados en prácticas y normas óptimas aceptadas internacionalmente utilizando tecnologías que garanticen la privacidad y la seguridad.
5. Los diseñadores de programas y equipos informáticos deben hacer todo lo posible para elaborar tecnologías fiables que promuevan la capacidad de recuperación y resistan a las vulnerabilidades.
6. Las autoridades gubernamentales deben participar activamente en los esfuerzos desplegados por las Naciones Unidas para promover la ciberseguridad y ciberpaz mundiales así como para evitar la utilización del ciberespacio con fines de conflicto.

En estos principios, especialmente del sexto, se reconoce la firme intención de encauzar los posibles conflictos en el ciberespacio. En efecto, dado el aspecto bélico de las actividades en el ciberespacio, tanto las autoridades gubernamentales como los responsables no gubernamentales deben hacer especial hincapié en la búsqueda de la ciberpaz, a la luz del crecimiento alarmante de las capacidades ofensivas de la "ciberguerra".

Estos problemas se tratan en forma más exhaustiva en otras partes de este libro. No obstante, en el presente contexto se contemplan algunas declaraciones de principio destinadas a aclarar el concepto de ciberespacio. Hasta el momento, el ciberespacio es, en muy gran medida, un espacio no reglamentado y a disposición de todos, sin directrices ni sanciones, y en el que, al parecer, está permitido actuar sin ningún tipo

de trabas de carácter jurídico. De ahí la necesidad de establecer códigos comunes de ciberconducta en todos los ámbitos de la actividad digital. Desde 2001, la Federación Mundial de Científicos ha pedido que se defina una ley universal del ciberespacio, preferiblemente bajo los auspicios de las Naciones Unidas.[125] En ningún aspecto es más pertinente que en el correspondiente a la utilización militar ofensiva del ciberespacio.

La complejidad de esta tarea y sus obstáculos jurídicos y, quizás ante todo, políticos, son evidentes. Como ya se ha indicado en otra parte de este libro, la legislación tradicional en materia de guerra y conflictos armados es ambigua e incluso de utilidad sumamente limitada, y se carece de definiciones. Las referencias a los límites tradicionales de la acción en los principales textos de derecho internacional, como los correspondientes a la Carta de la Naciones Unidas o al Tratado de la Organización del Atlántico Norte (OTAN) son en gran medida infructuosas. El texto principal de los Convenios de Ginebra y de algunas resoluciones y convenciones de la Asamblea General de las Naciones Unidas, por ejemplo, en el ámbito del delito transnacional organizado, el terrorismo o el comportamiento en el espacio ultraterrestre, permiten en el mejor de los casos analogías indirectas e incompletas.[126] El concepto de "control de armamentos" o los límites entre utilización lícita o "ilícita" de las TIC, o entre ataque y defensa, son vagos, dado que las tecnologías son idénticas y el problema del "doble uso" que padece el control de armamentos en tantos aspectos se vuelve, en este caso, endémico. Por otra parte, el dilema del seguimiento y localización, atribución de autoría de forma fiable y en periodos adecuados, que ya convierte en problemática la persecución del ciberdelito "simple", se ha profundizado en el dominio militar dada la probabilidad de que un atacante belicoso aplique al máximo las

---

125 Ver *Toward a Universal Order of Cyberspace: Managing Threats from Cybercrime to Cyberwar*, Informe y Recomendaciones, Grupo de Supervisión Permanente de la Federación Mundial de Científicos sobre la Sociedad de la Información, 19 de noviembre de 2003, presentación realizada en la Cumbre Mundial sobre la Sociedad de la Información, www.itu.int/dms_pub/itu-s/md/.../S03-WSIS-C-0006!!PDF-E.pdf.

126 Indirectas pero de ninguna manera insignificantes. *Ver* Sergei Komov, Sergei Korotkov, Igor Dylewski, "Military aspects of ensuring international information security in the context of elaborating universally acknowledged principles of international law", *ICTs and International Security*, Instituto de las Naciones Unidas de Investigación sobre el Desarme, 2007, www.isn.ethz.ch/isn/Current-Affairs/Security-Watch/Detail/?fecvnodeid=128420&dom=1&groupot593=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&fecvid=21&ots591=0c54e3b3-1e9c-be1e-2c24-a6a8c7060233&v21=128420&lng=en&id=47166.

técnicas más modernas de evasión y disimulo. La verificación, un ingrediente esencial del control de armamentos, es prácticamente imposible. La disuasión en su sentido tradicional no es viable puesto que han desaparecido sus requisitos básicos (atribución, lugar de origen, nivel de respuesta). Es por tanto lógico que las opiniones más expertas sostengan que apostar a la defensa del ciberespacio (haciéndola extensiva al ciberespacio de los aliados) y no a la disuasión en el ciberespacio *en sí* resulta la opción más adecuada.[127]

Sin embargo, si se tiene seriamente en cuenta el concepto de ciberespacio, es esencial contar con un marco jurídico para definir lo que constituye una violación de la paz, y los Estados no deberían quedar paralizados ante las imperfecciones inherentes a dicho marco. El Secretario General de la UIT, sin limitarse a los cinco principios de la UIT, ha sugerido que las naciones, en un documento de esa naturaleza, se comprometan a no ser las primeras en lanzar un ciberataque contra otra nación ("no atacar en primer lugar") y a no dejar impunes a ciberterroristas y atacantes en su país.[128] Por otra parte, se alienta a las naciones a concertar, de forma bilateral o multilateral, pactos de no agresión en el ciberespacio. Podrían establecerse compromisos mutuos de no atacar las infraestructuras nacionales básicas (especialmente las utilizadas con fines humanitarios o las que están al servicio de necesidades humanas fundamentales que, en parte, ya están protegidas por el derecho internacional actual) y confirmarse la inviolabilidad de las redes de datos transfronterizas. Constituiría un paso transcendental y de gran valentía deslegitimar, en un instrumento internacional, las ciberarmas ofensivas y las estrategias ofensivas para su utilización.

Seamos realistas: con toda probabilidad, este tipo de estrategias y principios cuya finalidad es fomentar la paz en el ciberespacio no contará con el apoyo espontáneo de numerosos países que ya han invertido mucho, y seguirán haciéndolo, en una posible ciberguerra, aprovechando el vacío jurídico actual en materia de ciberespacio. De hecho, los informes actuales sobre la sistemática "militarización" del ciberespacio, la creación de cibercomandos, la formulación de ciberestrategias ofensivas y otros no son nada tranquilizadores. Sin embargo, no hay que subestimar las implicaciones morales de las acciones multilaterales para contrarrestar este flagelo. La legitimidad es una herramienta importante del arte de gobernar, y el mero hecho de definir los límites de la acción, y de establecer y acordar criterios, podría ser motivo de impulso a medida que transcurra el tiempo. Para que contribuya a la ciberestabilidad y al

---

127 Ver, por ejemplo, Martin C. Libicki "Cyber deterrence and Cyberwar", Santa Mónica, 2009, pág. 158 y siguientes.

128 Ver Capítulo VII.

respeto de los derechos fundamentales, la paz en el ciberespacio necesita determinadas medidas de aplicación.

Hay razones poderosas en este sentido. El funcionamiento y la estabilidad de la estructura de la red mundial interdependiente, y la confianza depositada en ambos, constituyen un bien público de interés común. Los ciberataques generalizados, hasta en un solo segmento del sistema, son difíciles de controlar y sus consecuencias podrían ser incalculables; hay una tendencia intrínseca a desatar reacciones en cadena, incluso de acontecimientos modestos.[129] Ello podría alterar decisivamente las ecuaciones de poder, así como la estabilidad geocibernética de todo el entorno digital del que depende la sociedad, muy por encima de las meras partes en un conflicto. Todos los actores internacionales comparten el interés en el mantenimiento de las redes transnacionales y las estructuras de la información.

No es necesario ningún argumento para sostener que una ciberacción ofensiva no provocada, de hecho cualquier ciberataque, es incompatible con los principios de la paz en el ciberespacio.

Pero el concepto logra pasar su prueba decisiva cuando define y evalúa la *reacción* a los ataques en el ciberespacio, reales o esperados, en caso de ciberconflicto. Se entienda por ciberataque un ataque armado o no, o cuando se entienda de ambas maneras, hay un acuerdo general en el principio primordial de la legislación internacional relativo al derecho a la legítima defensa *en su sentido genérico* de legitimidad de la autoprotección e impedimento del ataque. Como se ha señalado en repetidas ocasiones en este libro, definir las acciones hostiles como "ataque armado" resulta, en términos de la Carta de las Naciones Unidas, el Tratado de la Organización del Atlántico Norte (OTAN) y el derecho internacional general, el factor necesario para propiciar la legítima defensa individual y colectiva *por medios militares.* Sin lugar a duda, se puede sostener que un ciberataque a otro Estado o con repercusiones en

---

129 "La comunidad internacional debe comprender que una pequeña escaramuza en el ciberespacio podría ser precursora de un importante ciberconflicto y desencadenar una escalada cinética regional que tendría repercusiones internacionales". Extraído de John Bumgarner, Chief Technology Officer, US Cyber Consequences Unit, *Jane's Defence Weekly*, 29 de septiembre de 2010, www.jdw.janes.com (en lo sucesivo, "Jane's").

otro Estado es un "ataque armado" o su equivalente, al menos cuando entrañe una gran destrucción o la pérdida importante de vidas humanas.[130]

Esto podría constituir el fundamento jurídico de la acción colectiva, incluso por medios militares. Pero, en el contexto de la tecnología digital, la definición y oportunidad de la acción de represalia militar requiere una nueva y detenida reflexión y, por último, una política de contención deliberada.

Las diferencias entre ciberconflicto y "guerra" tradicional -cinética- son sorprendentes y no se limitan a la diferencia evidente del "armamento" utilizado. Como resumen de los argumentos esgrimidos en otras partes de este libro, e incluso en este mismo capítulo, podemos indicar, en primer lugar, la incertidumbre en la atribución, y los niveles de atribución, de la autoría de los ciberataques, lo cual hará incierto el destinatario de cualquier contramedida o represalia. ¿Contra quién podrá estar legítimamente dirigida? No hay que olvidar, además, la omnipresencia e interconexión de los sistemas y redes digitales, la imprevisibilidad de las consecuencias de las contramedidas digitales y, por consiguiente, la dificultad del crecimiento gradual de cualquier contramedida. En tercer lugar, los conflictos en el ciberespacio pueden generar ataques sumamente coordinados y, por tanto, de consecuencias catastróficas, o adoptar la forma de una situación implícitamente generalizada de amenazas perpetuas de bajo nivel (ciberespionaje, creación de redes robots no reconocidas, etc.) con distintos grados de posibilidad de que entrañen una desintegración de infraestructuras con consecuencias de vasto alcance. En el contexto de un conflicto entre Estados, se observa además una novedad: la presencia de un número infinito de posibles actores. Las enseñanzas de la Guerra Fría de la segunda mitad del siglo pasado, el funcionamiento de un equilibrio militar-nuclear entre dos potencias, con su combinación singular de disuasión y contención, sencillamente no pueden trasladarse a un escenario con numerosos actores hostiles. Por último, como ya se ha señalado, hay que tener en cuenta el interés común de todos en el mantenimiento de una infraestructura mundial de la información en pleno funcionamiento.

Estas diferencias, y otras que podrían citarse, deben orientar nuestro modo de pensar con respecto a las respuestas a los ataques. En el marco del concepto de paz en el

---

130 Mientras se redactaba este texto, los países de la OTAN, en preparación de una reunión cumbre de los Estados integrantes del Tratado de Washington (20 de noviembre de 2010), contemplaban la adopción de decisiones colectivas ante nuevas amenazas, incluidos los ciberataques. Si los ciberataques se incluyen en la adopción de decisiones en materia de defensa colectiva, se aplicarán el Art. 4 (consultas mutuas) y el Art. 5 (asistencia mutua mediante la adopción de medidas "que se estimen necesarias, incluida la utilización de la fuerza armada").

ciberespacio, se debe dar prioridad al mantenimiento o pronto restablecimiento de un entorno pacífico y estable, lo cual apunta, sin ninguna duda, a la defensa.

La autodefensa preventiva es el elemento esencial de las respuestas compatibles con la paz. Bajo este concepto, se debe reconocer la responsabilidad común de todos los interesados en el mundo digital de utilizar redes y sistemas seguros, requisito también estipulado en la Declaración Erice. La colaboración entre empresas y autoridades gubernamentales es tan importante como la cooperación internacional. El término clave es resistencia: no sólo la calidad de los sistemas sino también su gestión deben contribuir a la solidez e impermeabilidad ante los ataques. Los interesados deberán optimizar el conocimiento real de sus redes, identificar las ventajas de gran valor y resolver sus vulnerabilidades (seguimiento en tiempo real de toda la red, establecimiento de zonas de seguridad, segmentación de la red, garantía de la seguridad de la energía). Por consiguiente, se debe disponer con facilidad de sistemas y programas resistentes que respeten rigurosamente los protocolos y normas de la UIT así como la seguridad nacional. La resistencia de las infraestructuras de las tecnologías de la información desalienta los ataques y contribuyen a un entorno pacífico. Un grado elevado de defensa constituye un elemento esencial de la estabilidad en el ciberespacio dado que impide los ataques y, al mismo tiempo, contribuye a dar confianza y ofrece tranquilidad a los operadores.

La resistencia, según su definición general, incluye varios elementos, entre ellos la calidad de autorecuperación de los sistemas y la disponibilidad de sistemas de alerta y componentes redundantes integrados, pero también modos de comportamiento como la exploración de ámbitos de cooperación con la comunidad de interesados en un entorno pacífico y el aumento del intercambio de información; en otras palabras, se debe poner el acento en la acción positiva y en el estímulo de llevarla a la práctica. En los Estados que examinan, y desean contrarrestar, posibles situaciones de ciberconflicto, se podrían considerar también actividades de alto nivel en materia de reglamentación como, por ejemplo, acuerdos de no agresión en el espacio cibernético, acuerdos de transparencia para desactivar imágenes del enemigo, supervisión de actos malintencionados e intercambio de información, todas ellas actividades que permitan identificar mejor a los autores en caso de conflicto. Varias de estas propuestas se han incluido en la propuesta anteriormente citada del Secretario General de la UIT. El incipiente mecanismo de alerta temprana mundial (el Centro de Respuesta Global (CRG), el sistema de alerta temprana de la red (NEWS) o ESCAPE) reviste indudablemente gran interés puesto que permite dar respuestas no violentas. Los marcos de cooperación internacional deben utilizar redes CERT cada vez más amplias.

Sin embargo, hay que tomar disposiciones con respecto a situaciones graves de ciberconflicto cuando una simple posición de defensa pasiva no es suficiente y se debe invocar en forma activa el derecho a la autodefensa en virtud del derecho internacional. Desde la perspectiva de la paz en el ciberespacio, tampoco aquí sería conveniente establecer simples analogías con la legislación tradicional en materia de conflictos armados. Se corre el riesgo de que el marco mental así creado dé lugar a contextos bélicos de represalia militar y a la lógica militar de la destrucción máxima de los bienes del enemigo. El recurso a reglas de compromiso heredadas podría dar resultados peligrosos. La ciberpaz no implica renunciar íntegramente a contramedidas ofensivas ni a represalias, pero sí no olvidar de manera alguna los matices de los contextos aplicables.

El término esencial en la elaboración de respuestas será *contención.* Sus elementos contemplarán un análisis riguroso y permanente de las amenazas y riesgos para evitar consecuencias incontrolables con respecto a la disfunción global de las redes cibernéticas; la concentración de respuestas bien elegidas y sin crecimiento gradual; la paciencia y oportunidad en dar la respuesta con miras a permitir una mejor imputabilidad del ataque y la activación de sistemas de redundancia y alianzas de defensa entre pares; el cuidado meticuloso en la aplicación de los principios de proporcionalidad y necesidad inherentes del recurso a la autodefensa y, por último, la protección cuidadosa de las infraestructuras básicas de carácter humanitario o socialmente indispensables.

Aunque probablemente sería exagerado afirmar que en las respuestas a los ciberataques, la defensa es *siempre* el mejor ataque, la paz en el ciberespacio, en el presente análisis, parece exigir, junto con los límites estrictos a las represalias, el principio de dar mayor prioridad a la autodefensa que al ataque.[131]. Este principio estaría en armonía con el llamamiento a una deslegitimación sistemática de las "armas" utilizadas en el ciberespacio y de las ciberestrategias ofensivas en el plano estatal, como se ha señalado anteriormente.

---

131 "Clausewitz no pudo prever que el mejor ataque del siglo XXI consistiría en una firme defensa del ciberespacio". Jane's.

7 Respuesta internacional a la ciberguerra

Por Hamadoun I. Touré

7.1 Políticas y planteamientos nacionales

Los países de todo el mundo responden de diversas maneras a la nueva amenaza de la ciberguerra. Si bien algunos Estados apenas empiezan a abordar la cuestión de la ciberseguridad[132], la mayoría de los gobiernos reconocen al menos que es necesario reasignar recursos y reformar hasta cierto punto las estrategias nacionales de seguridad. Muchos países están aumentando los recursos financieros, de investigación, tácticos y diplomáticos para mejorar su ciberseguridad[133]. Algunos países crean "cercos de aire" (*air gap*) para tratar de aislar determinadas redes impidiendo que se conecten con otros sistemas, a fin de proteger estructuras y sistemas esenciales de la información contra ataques[134]. A continuación se evalúan los distintos sistemas adoptados por varios Estados.

a) Incorporación de cibercapacidades en la estrategia bélica convencional

Varios países están estudiando planteamientos bélicos convencionales en relación con sus cibertácticas, así como la creación de ciberarmas con capacidades ofensivas y defensivas. Consideran que las armas cibernéticas son "multiplicadores de fuerza" que se utilizarán principalmente en acciones bélicas tradicionales para aumentar notablemente su potencial bélico[135]. Durante estos últimos años Internet se ha convertido en un importante medio de intercambio de información y propaganda durante los conflictos armados. A este respecto, muchos países consideran que el

---

132 Por ejemplo, Sudáfrica sólo anunció recientemente (Feb. 2010) su intención de comenzar a formular una política nacional coordinada de ciberseguridad. "Notice of Intention to Make South African Cybersecurity Policy", Republic of South Africa, Government Gazette, Nº 32963, 19 de febrero de 2010, www.pmg.org.za/files/docs/100219cybersecurity.pdf.

133 "Cyberwar: Sabotaging the System – 60 Minutes – CBS News", 8 nov. 2009, www.cbsnews.com/stories/2009/11/06/60minutes/main5555565.shtml (en el cual se informa de que el Congreso de EE.UU. ha asignado 17.000 millones USD para iniciativas de ciberseguridad ofensivas y defensivas).

134 David Eshel, "Israel Adds Cyber-Attack to IDF", Military.com, 10 de febrero de 2010, www.military.com/features/0,15240,210486,00.html (en adelante "Eshel").

135 Kevin Coleman, "Russia's Cyber Forces", DefenseTech, 27 de mayo de 2008, http://defensetech.org/2008/05/27/russias-cyber-forces/.

sabotaje de información en Internet es una agresión militar contra la moral pública y, por lo tanto, están dispuestos a recurrir a la fuerza militar para luchar contra los ciberataques[136]. Las recientes filtraciones de documentos militares confidenciales ilustran por qué los Estados se preocupan por las posibles consecuencias de las cibervulnerabilidades para la moral y el apoyo públicos[137]. Varios funcionarios públicos ya han señalado que consideran que las tácticas bélicas informáticas son acciones militares, ocasionen o no pérdidas humanas, y que por consiguiente justificarían una respuesta militar[138].

b) Cultivar las cibertácticas como recurso nacional

Mediante la redistribución de recursos y fondos y la reorientación de la planificación estratégica, muchos países tratan su infraestructura digital y las TIC como recursos nacionales o activos estratégicos. Algunos países incluso han articulado explícitamente esta redistribución como nueva política nacional[139]. Algunos países han transferido recursos presupuestarios a iniciativas ciberespaciales y reservado sumas considerables para capacidades de investigación y desarrollo de capacidades bélicas cibernéticas[140]. Varios gobiernos han articulado y comenzado a perseguir planes nacionales integrados para afrontar las nuevas amenazas cibernéticas, movilizando múltiples sectores y

---

136 Gregory Asmolov, "Russia: New Military Doctrine and Information Security", Global Voices, 23 feb. 2010, http://globalvoicesonline.org/2010/02/23/russian-military-doctrine/ (descripción de la doctrina militar modernizada de Rusia, en la que la guerra informática se considera una agresión militar).

137 Véase, por ejemplo Jo Biddle, "AFP: Huge leak of secret files sows new Afghan war doubts", 27 de julio de 2010, www.google.com/hostednews/afp/article/ALeqM5gZkjOIqwM0xJDr0u5fPrc5rxdEQg.

138 Cyberwarfare, Congressional Research Service, RL30735, Updated 19 June 2001, www.fas.org/irp/**crs**/RL30735.pdf (se cita a un oficial ruso que descartó la posibilidad de clasificar la guerra informática como no militar). Véase también Peter Beaumont, "US appoints first cyberwarfare general," Guardian.co.uk, 23 de mayo de 2010, www.guardian.co.uk/world/2010/may/23/us-appoints-cyber-warfare-general/ (se informa de que Estados Unidos también ha indicado que podría contemplar la posibilidad de recurrir a tácticas militares convencionales para responder a ciberataques) (en adelante "Cibergeneral").

139 Presidente Barack Obama, "Remarks by the President on Securing Our Nation's Cyber Infrastructure", The White House, 29 may. 2009, www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure (se indica que la infraestructura digital del país se considerará en adelante un "activo nacional estratégico" y que su protección será una "prioridad de seguridad nacional").

140 Irán (se estima que el presupuesto ciberbélico de Irán es de aproximadamente 76 millones USD).

transformando completamente recursos y estrategias[141]. Este tipo de transformación puede comprender la capacitación (o formación profesional continua) de personal militar, mediante una modernización de los servicios de inteligencia para dedicarse principalmente a la compilación de información científica y tecnológica pertinente y llevar a cabo simulaciones de ciberguerra y ejercicios militares, prestando siempre una atención específica a las aplicaciones informáticas[142]. Varios países han lanzado concursos nacionales para identificar y contratar a los mejores cerebros informáticos civiles nacionales[143]. También se incita a las empresas nacionales a desarrollar mejores capacidades técnicas para apoyar la nueva estrategia militar. Algunos gobiernos también tratan de mantener un grupo de piratas civiles privados a los que puedan recurrir en caso de necesidad[144]. Estos "piratas activistas" pueden ser personas expertas en informática o incluso antiguos piratas ilegales contratados y formados para que utilicen sus conocimientos al servicio de la seguridad nacional[145]. Otros países incluso recurren a representantes, piratas mercenarios y especialistas de otros países que actúan en su nombre[146]. Todos estos cambios demuestran una evolución con respecto a estrategias más reactivas ante las amenazas informáticas y una reorientación en torno a la elaboración de tácticas bélicas informáticas proactivas para actuar eficazmente en condiciones de alta tecnología[147].

---

141 Gurmeet Kanwal, "China's Emerging Cyber War Doctrine", p. 20, Journal of Defense Studies, 2009, en: www.idsa.in/system/files/jds_3_3_gkanwal_0.pdf (se examina la política china en materia de guerra informática y acupuntura) [en adelante "Kanwal"].

142 Cyberwarfare: An Analysis of the Means and Motivations of Selected Nation States, Dartmouth College, Institute for Security, Technology, and Society, nov. 2004, p. 2, www.ists.dartmouth.edu/docs/execsum.pdf (en adelante "naciones seleccionadas").

143 Véase p.ej. Richard Westcott, "UK Seeks Next Generation of Cybersecurity Specialists", BBC News, 26 jul. 2010, www.bbc.co.uk/news/technology-10742588.

144 Kanwal p. 20.

145 Gordon Corera, "Cyber-security strategy launched", BBC News, 25 jun. 2009, http://newsvote.bbc.co.uk/mpapps/pagetools/print/news.bbc.co.uk/2/hi/uk_news/politics/8118348.stm?ad=1 (en adelante "Corera"); Tom Gjelten, "Cyberwarrior Shortage Threatens U.S. Security", National Public Radio, 19 jul. 2010, www.npr.org/templates/story/story.php?storyId=128574055.

146 Eshel.

147 Kanwal p. 20.

c) Creación de equipos militares cibernéticos

Varios países han respondido a la nueva amenaza de la ciberguerra atribuyendo numerosas tropas militares al combate virtual[148]. Este cambio de política podría entrañar la creación de equipos bélicos en Internet, que podrían estar integrados en otros organismos de inteligencia[149], o incluso la creación dentro de la estructura militar de sectores completamente nuevos dedicados a actividades cibernéticas[150]. Estos nuevos equipos militares integrarán y prepararán recursos militares para operaciones en todo el ciberespacio[151]. Si bien se dedican principalmente a la protección de redes militares y a la realización de operaciones militares en el ciberespacio, también se les puede encomendar la seguridad de las redes privadas que sustentan partes considerables de numerosas operaciones militares[152].

d) Utilización de cibertácticas para nivelar el campo de batalla

Al perfeccionar sus tácticas bélicas informáticas y electrónicas, algunos países esperan nivelar el campo de batalla con países que recurren a programas y equipos informáticos para movilizar sus fuerzas armadas convencionales. Esta transición entraña inversiones en nuevos sistemas de mando automatizados, incluidos materiales como cables de fibra óptica, satélites y sistemas radioeléctricos digitales de alta frecuencia, así como una mayor atención a los sistemas de vigilancia espacial,

---

148 Algunos países han revelado grandes cambios de personal. Véase Cibergeneral (en el que se indica que Estados Unidos anunció la reasignación de 30.000 soldados al cibercombate). En cambio, es más difícil acceder a información sobre las estrategias de muchos otros países. Véase Robert McMillan, "Black Hat Talk on China's 'Cyber Army' Pulled After Pressure", InfoWorld, 15 jul. 2010, www.infoworld.com/print/130362.

149 Eshel.

150 Por ejemplo, Estados Unidos anunció la creación de una nueva unidad cibermilitar en 2009. Cibergeneral. El Reino Unido también anunció recientemente la creación de un centro de operaciones de ciberseguridad en el marco de su estrategia de ciberseguridad. Corera.

151 Véase "U.S. Cyber Command Fact Sheet", U.S. Department of Defense, 25 may. 2010, www.defense.gov/home/features/2010/0410_cybersec/docs/CYberFactSheet%20UPDATED%20replaces%20May%2021%20Fact%20Sheet.pdf.

152 Siobhan Gorman, "U.S. Backs Talks on Cyberwarfare", The Wall Street Journal, 4 jun. 2010, http://online.wsj.com/article/SB10001424052748703340904575284964215965730.html (se observa que 90% de la potencia militar estadounidense procede del sector privado, según oficiales del ejército estadounidense) (en adelante "Gorman").

aérea, naval y terrestre[153]. Algunos gobiernos ya utilizan las TIC y personal militar experto en informática para vigilar sus fronteras nacionales[154]. Las nuevas estrategias informáticas podrían depender aún más de esos recursos y de los correspondientes sistemas automatizados para proteger las fronteras. Otras tácticas podrían consistir en operaciones de mando y control destinadas a perturbar la circulación de información del enemigo y en la deterioración y destrucción de máquinas, redes y datos esenciales de las infraestructuras TIC del enemigo[155]. Estos cambios tienen por objeto atacar los puntos débiles de posibles adversarios, es decir, los que dependen del ciberespacio y de nuevas tecnologías. Es posible que los países que tienen las mayores capacidades bélicas tradicionales y cibernéticas sean los más vulnerables a causa de la tecnología que los fortalece, y que puede ser más vulnerable a nuevos tipos de ataques como bombas lógicas y el pirateo[156]. Los países sacan partido de la posible asimetría de las acciones en el ciberespacio y esperan neutralizar así las capacidades militares de sus adversarios[157].

e) Educación de los ciudadanos y sensibilización sobre los problemas de ciberseguridad

Muchos gobiernos reconocen que la información y la sensibilización del público son métodos muy útiles de defensa informática[158]. Las bases de datos de información y los meses de sensibilización nacionales organizados por gobiernos o entidades privadas

---

153 Kanwal p. 16.

154 Kanwal p. 14.

155 Kanwal p. 18.

156 Radical Change ("Because the United States is the most Internet-dependent and automated... it's also the most vulnerable to cyberattack.").

157 Kanwal p. 18; CRS Cyberwarfare p. 11.

158 Véase por ejemplo Naciones seleccionadas, p. 5 (se recomiendan esfuerzos sistemáticos y sostenidos para cambiar la opinión del pueblo estadounidense sobre la seguridad de las redes, a fin de mejorar la ciberseguridad nacional).

ayudan a aumentar la sensibilización de manera radical[159]. Estos programas están destinados a menudo a informar a usuarios y pequeñas empresas sobre cómo proteger su información y sus sistemas contra ciberdelitos tales como el robo de identidad y el pirateo. En la mayoría de los casos, el acceso ilegal a sistemas informáticos son sólo es una primera etapa esencial, y el pirateo de ordenadores o sistemas informáticos puede ser precursor de otros delitos que afectan a la seguridad nacional, tales como el espionaje de datos o la denegación de servicio. Cuando están dirigidos contra recursos nacionales esenciales u órganos públicos, quizá sea más apropiado calificar esos "delitos" de ciberataques o ciberguerra. Los piratas ya tratan sistemáticamente de infiltrar entidades públicas, empresas privadas y sistemas de defensa nacional, con un éxito considerable[160]. El espionaje de datos o el acceso a información confidencial se puede lograr con medios técnicos o métodos de "ingeniería social", una táctica que consiste en engañar a personas para obtener acceso a sistemas que normalmente son seguros[161]. Por consiguiente, la información del público sobre la utilización de métodos técnicos y de ingeniería social, como dejar memorias USB infectadas en lugares públicos, puede ayudar a proteger recursos nacionales[162].

f) Países menos conectados y en desarrollo

Muchos países dependen considerablemente de las TIC y de Internet para sus infraestructuras y servicios esenciales, mientras que otros países no dependen tanto de esas tecnologías y utilizan redes internas nacionales o recursos distintos de las TIC. Ahora bien, incluso esos países parecen estar aumentando sus capacidades en línea,

---

159 Por ejemplo, la Junta Informática Nacional de Mauricio, en el ámbito de su Ministerio de Tecnologías de la Información y la Comunicación, supervisa un portal de sensibilización sobre ciberseguridad, en www.gov.mu/portal/sites/ncbnew/main.jsp, y en Estados Unidos todos los meses de octubre son el mes nacional de sensibilización sobre ciberseguridad. Asociaciones público-privadas, como la National Cybersecurity Alliance de EE.UU., también informa a usuarios y administradores de la infraestructura digital sobre cómo crear sistemas resistentes y mecanismos de protección. Véase "About Us", The National Cybersecurity Alliance, www.staysafeonline.org/content/about-us.

160 Véase por ejemplo Understanding p. 20 (lista de objetivos famosos de varios ataques piratas, comprende entre otros al Pentágono, el gobierno de Alemania, Google, Ebay y NASA). **UIT -esta cita no se ha visto antes. Se necesita la cita completa.**

161 Véase id. p. 23–24.

162 Por ejemplo, el mando central de EE.UU. fue infiltrado en 2008 por medio de una memoria USB infectada. Véase Fifth Domain.

aunque los avances pueden limitarse a utilizaciones militares o gubernamentales[163]. Los países que se han informatizado más recientemente son menos vulnerables a los ciberataques, ya que sus sistemas públicos integrados comparten menos conexiones con el resto del ciberespacio[164]. Aun así, incluso los países en desarrollo que todavía no disponen de la infraestructura necesaria para aprovechar todos los beneficios de las TIC todavía dependen de Internet y de otras tecnologías móviles y digitales para atender a algunas de sus necesidades esenciales[165] y, por consiguiente, también se interesan por el futuro de la ciberseguridad.

7.2 Respuestas internacionales recientes

Hoy los esfuerzos internacionales para afrontar la amenaza de la ciberguerra son mucho menos numerosos que las estrategias nacionales, aunque se han probado varias iniciativas multilaterales. También se han probado planteamientos bilaterales, pero éstos distan mucho de ser una estrategia completa para mejorar la ciberseguridad y garantizar la ciberpaz, ya que sólo interviene una escasa proporción de los actores interesados en la ecuación de la ciberpaz. Algunos países han solicitado la creación de un tratado para limitar la utilización de ciberarmas, mientras que otros han insistido en que ese tratado es innecesario o prematuro[166]. Estas propuestas pueden ser un primer paso hacia la colaboración internacional, pero también distan de un planteamiento realmente global y de una estrategia clara para seguir avanzando, en la que participen todos los interesados. A continuación se presenta una lista no exhaustiva de varias respuestas internacionales recientes.

a) Comisión de Prevención del Delito y Justicia Penal (CPDJP) de la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD)

En abril de 2010, el 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal (CPDJP) redactó una serie de declaraciones que comprendía una

---

163 Martyn Williams, "North Korea Moves Quietly Onto the Internet", Computerworld, 10 de junio de 2010, www.computerworld.com/s/article/9177968/North_Korea_moves_quietly_onto_the_Internet.

164 Corera.

165 Véase por ejemplo, "Economic and Social Council Opens General Segment of 2010 Session", p. 3, ECOSOC/6444, 16 jul. 2010, www.un.org/News/Press/docs/2010/ecosoc6444.doc.htm (se estudia el "dinero digital" o sistema de moneda electrónica utilizado en países africanos) (en adelante "ECOSOC 2010").

166 Gorman.

disposición en la que se pedía que un grupo de expertos intergubernamental estudiara el problema del ciberdelito y las respuestas internacionales al mismo[167]. En consecuencia, durante la 19ª reunión de la Comisión de Prevención del Delito y Justicia Penal, sus Estados Miembros formularon la Recomendación conexa en la que piden que la Comisión establezca un Grupo intergubernamental de expertos de composición abierta encargado de llevar a efecto esa disposición del CPDJP[168]. El Congreso no logró un consenso sobre la preparación de un nuevo tratado sobre el ciberdelito, pero alcanzó varios acuerdos sobre asistencia técnica y creación de capacidades que ya constituye una base apropiada para los debates sobre medidas futuras[169].

b) Consejo Económico y Social de las Naciones Unidas (ECOSOC)

El Consejo Económico y Social de las Naciones Unidas (ECOSOC) inició su periodo de sesiones de 2010 con una sesión de información sobre las dificultades que plantea la ciberseguridad, así como las amenazas que plantea y las oportunidades que ofrece la siempre creciente utilización de Internet. Entre otras cosas, el Consejo insistió en la necesidad de llevar a cabo iniciativas internacionales en las que se contemplen intercambios de información, prácticas idóneas, capacitación e investigación. Además, los panelistas declararon que las Naciones Unidas deben estar "unidas en la acción" al respecto, lo cual debe aumentar la cooperación entre los países y también la colaboración entre los Estados y el sector privado para garantizar la ciberseguridad[170]. Advirtieron que el alcance internacional y las funestas consecuencias de una ciberguerra real exigen una respuesta coordinada; las soluciones ad hoc y el fortalecimiento de las defensas son ahora estrategias inapropiadas[171].

---

167 "Proyecto de Declaración de Salvador sobre estrategias amplias ante problemas globales: los sistemas de prevención del delito y justicia penal y su desarrollo en un mundo en evolución", Declaración 42, 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, 18 abr. 2010, www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/In-session/ACONF.213L6_Rev.2/V10529031A_CONF213_L6_REV2_E.pdf.

168 "Informe del 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal", ONUDD, Salvador, Brasil, 12–19 abr. 2010, www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf.

169 "Resumen de resultados sobre el delito cibernético: 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal", Proyecto sobre delitos cibernéticos, 26 abr. 2010, www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/2079_UNCC_cyberoutcome.pdf.

170 ECOSOC 2010.

171 Id. (estudio del "dinero digital", sistema de dinero electrónico utilizado en países africanos).

c) Organización del Tratado del Atlántico Norte (OTAN)

En 2008 la OTAN implementó su propia política de ciberdefensa a fin de proteger sus recursos tecnológicos y los de sus países miembros[172]. En el marco de esa política la alianza creó una Autoridad de gestión de ciberdefensa, una Capacidad de respuesta a incidentes informáticos, que se encarga del envío de equipos de refuerzo rápido a los países miembros, y un Centro de Excelencia sobre ciberdefensa cooperativa[173]. El Centro, ubicado en Estonia, alberga a expertos que realizan actividades de investigación y capacitación sobre ciberseguridad. Lo financian países como Estonia, Letonia, Lituania, Alemania, Italia, la República Eslovaca y España[174].

Además, la OTAN ha organizado ejercicios de ciberdefensa en los que equipos de estados miembros tratan de defender redes informáticas virtuales contra ciberataques. Esos ejercicios tienen por objeto aumentar la comprensión de la informática internacional y mejorar la cooperación internacional en el tratamiento de incidentes técnicos[175]. La OTAN también ha firmado Memoranda de Entendimiento relacionados con la ciberseguridad con Estonia, Estados Unidos, el Reino Unido, Turquía y Eslovaquia[176].

d) Consejo de Europa – Convenio de Budapest sobre la Ciberdelincuencia

El Convenio del Consejo de Europa sobre la Ciberdelincuencia[177] de ciertos ciberdelitos indica disposiciones legales modelo que los países pueden adoptar y adaptar a sus necesidades específicas. El Convenio trata de ciertas soluciones legales a delitos como el acceso ilegal (pirateo) y la intercepción, pero no aborda algunas de las incursiones informáticas más amenazadoras tales como el espionaje y el sabotaje de datos. Por otra parte, a pesar de que el Convenio trata de fomentar la cooperación internacional criminalizando ciberdelitos básicos, su carácter preceptivo está limitado

---

172 "Defending Against Cyber Attacks", NATO, www.nato.int/cps/en/natolive/topics_49193.htm.

173 "NATO 2020", www.nato.int/cps/en/natolive/official_texts_63654.htm?selectedLocale=en.

174 Cooperative Cyber Defense Center for Excellence, www.ccdcoe.org/.

175 "Defence exercise to boost skills for countering cyber attacks", NATO-News, 10 may. 2010, www.nato.int/cps/en/SID-012B6A76-D60B9579/natolive/news_63177.htm.

176 "NATO and Estonia conclude agreement on cyber defense", NATO-News, 23 abr. 2010, www.nato.int/cps/en/natolive/news_62894.htm.

177 Convention on Cybercrime CETS no.: 185, Consejo de Europa , http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=&DF=&CL=ENG (última visita 10 ag. 2010 (en adelante "Convention").

por la voluntad de sus redactores de no infringir otras posibles legislaciones nacionales. Las considerables diferencias culturales y legislativas lentifican o incluso impiden totalmente la adopción de una legislación unificada con arreglo a este planteamiento[178]. Apenas treinta países han ratificado el tratado desde que se abriera a la firma en noviembre de 2001, y sólo uno de ellos no es europeo[179].

Las disposiciones legislativas como las que figuran en el Convenio constituyen una posibilidad de afrontar algunas de las amenazas contra la ciberseguridad nacional e internacional. Ahora bien, las disposiciones del Convenio no tratan directamente de la cuestión de la ciberguerra entre países. Si bien la amenaza de sanciones puede disuadir a algunos aspirantes a ciberdelincuente, este tipo de legislación podría no ser suficiente para disuadir a los agresores que confían en que pueden evitar que los detecten, identifiquen o persigan.

e) Acuerdos bilaterales sobre ciberseguridad

Los Estados tratan asimismo de entablar relaciones con otros países en materia de ciberseguridad. Por ejemplo, el Ministerio de Comunicaciones y Tecnologías de la Información de India colabora con muchos países por medio de Memoranda de Entendimiento u otros esfuerzos de desarrollo y compartición de información. Por ejemplo, en 2004 India y Corea del Sur firmaron una declaración conjunta sobre cooperación bilateral en materia de tecnología de la información (TI) y el Equipo de respuesta a emergencias informáticas de la India también firmó un Memorándum de Entendimiento con el Centro nacional de ciberseguridad de Corea a fin de establecer una cooperación oficial sobre, entre otras cosas, ciberseguridad[180]. La India tiene además varios otros acuerdos bilaterales relacionados con las TI en general y otros que tratan específicamente de ciberseguridad y ciberdelincuencia[181].

---

178 "National Security Threats in Cyberspace", American Bar Association, Standing Committee on Law and National Security and National Strategy Forum, sept. 2009 p. 13, www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf (en adelante "Workshop").

179 Convention.

180 "Bilateral Cooperation: Asia", Departamento de Tecnologías de la Información de la India, Ministerio de Comunicaciones y TI del Gobierno de la India, www.mit.gov.in/content/bilateral-cooperation (en adelante "Cooperación").

181 Por ejemplo, la colaboración de la India con Brunei, Malasia, Francia y Australia se centra específicamente en la seguridad de la información y/o la ciberdelincuencia, mientras que otras relaciones se centran en aquel desarrollo de recursos e instalaciones. Cooperación.

Marruecos y Malasia también firmaron un Memorándum de Entendimiento sobre ciberseguridad durante la Conferencia regional sobre ciberseguridad que se celebró en Marruecos a principios de este año[182]. Este Memorándum creó una relación de cooperación entre los ministerios de ciberseguridad de ambos países y abarca temas tales como protección de infraestructuras esenciales de la información, desarrollo de marcos de ciberseguridad, creación de capacidades, capacitación y sensibilización. Es posible que estos tipos de colaboración mejoren la ciberseguridad de un país, pero no son suficientes para proteger a cualquier país contra una ciberguerra mundial. Por consiguiente, debe adoptarse una estructura mundial más completa relacionada con la ciberseguridad a fin de garantizar la paz para todos los países.

f) Unión Internacional de Telecomunicaciones (Comisión de Estudio 17 del UIT-T) –Normas mundiales

Con miras a analizar el creciente problema de la ciberseguridad, en particular en relación con las redes eléctricas inteligentes, la UIT ha creado un Grupo Temático sobre las redes eléctricas inteligentes que compilará documentada información y conceptos que podrían ser útiles para elaborar Recomendaciones en las que se aborden las redes eléctricas inteligentes desde una perspectiva de telecomunicaciones[183]. Los Grupos Temáticos son un instrumento de la UIT que completa el programa de trabajo de las Comisiones de Estudio ofreciendo un entorno de trabajo alternativo para la rápida elaboración de especificaciones en su ámbito de competencia[184]. Actualmente se recurre considerablemente a esos Grupos Temáticos para estudiar las necesidades del sector privado según van apareciendo, ya que son ideales para las tecnologías rápidamente cambiantes y evolutivas tales como las redes eléctricas inteligentes. El Grupo Temático sobre redes eléctricas inteligentes está integrado por representantes de varios Estados Miembros y colaborará con el sector mundial de las redes inteligentes (por ejemplo, institutos de investigación, foros, academias). Con miras a alcanzar su objetivo de elaborar Recomendaciones sobre normas para las redes eléctricas inteligentes, el Grupo Temático mantendrá una lista permanente de los organismos de normalización que tratan de redes eléctricas inteligentes, compilará opiniones y evaluará propuestas de redes eléctricas inteligentes, proporcionará las listas terminológicas y taxonómicas necesarias para las

---

182 "Malaysia and Morocco Are Now Partners in Cybersecurity", CyberSecurity Malaysia, 24 de enero de 2010, www.cybersecurity.my/data/content_files/44/632.pdf?.diff=1265036362.

183 Más información sobre el Grupo Temático en www.itu.int/ITU-T/focusgroups/smart/.

184 Grupos Temáticos del UIT-T en www.itu.int/ITU-T/focusgroups/.

redes eléctricas inteligentes, compilará nuevas ideas relacionadas con las redes eléctricas inteligentes e identificará posibles ámbitos de estudio correspondientes, y determinará las posibles consecuencias de la elaboración de normas en cuestiones tales como seguridad, privacidad e interfuncionamiento[185]. Todas esas actividades constituirán un enfoque integral y multifacético de las crecientes y rápidamente cambiantes dificultades de ciberseguridad relacionadas con las redes eléctricas inteligentes.

Además, gracias a sus contactos con el Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T), una de las organizaciones de normalización de las telecomunicaciones más reconocidas, el Grupo Temático podrá servir de fuente unificadora si hablan de información y orientación, respaldada por una reputación de normalización consensual de calidad. Las relaciones con el UIT-T también crean un entorno propicio para la progresión, en su caso, de los productos del Grupo Temático a través de la Comisión de Estudio como Recomendaciones, Suplementos, Manuales, etc., del UIT-T. Al formar parte del UIT-T, el Grupo Temático podrá lograr una mayor aceptación de sus especificaciones en muchos mercados mundiales y, en particular, en los países en desarrollo y en regiones que no participan muy activamente en el foro en cuestión.

7.3 Necesidad de un marco internacional

a) La disuasión no es viable

Todas las nuevas actividades humanas plantean nuevas dificultades. En tierra, mar, aire y espacio siempre se han planteado cuestiones de atribución, eficacia de utilización y solución de controversias que siguen planteándose hoy, y lógicamente el ciberespacio crea nuevos obstáculos y dilemas. La ciberseguridad afecta a todos los que están conectados y, habida cuenta de la creciente dependencia de las TIC para la infraestructura social básica, ahora afecta incluso a los que no están conectados. Los ataques contra la infraestructura de la información y los servicios Internet pueden llegar a causar nuevos graves daños a la sociedad. Habida cuenta de las características y dificultades particulares de la ciberguerra, es probable que ya no sean eficaces las antiguas estrategias probadas y comprobadas de mantenimiento de la paz.

---

185 Mandato del Grupo Temático del UIT-T sobre redes eléctricas inteligentes en www.itu.int/ITU-T/focusgroups/smart/tor.html.

La disuasión es desde hace mucho tiempo el método favorito para mantener la paz y la seguridad entre los países frente a armas de destrucción masiva. La eficacia de la disuasión depende sin embargo de determinadas circunstancias e hipótesis, que en muchos casos no se aplican en el ciberespacio[186]. La eficacia de la disuasión suele depender de cuatro elementos fundamentales: atribución (saber quién es el atacante), ubicación (saber de dónde partió del ataque), respuesta (poder responder, aun cuando se es víctima del primer ataque) y transparencia (el enemigo es conocedor de su capacidad e intención de responder con fuerza contundente)[187]. El ciberespacio y la ciberguerra plantean nuevos problemas que socavan la hipótesis fundamental de que esos cuatro elementos existen cuando los países crean sus arsenales de defensa militar. Las TIC aumentan las posibilidades que tiene el atacante de ocultar su identidad y ubicación. Puede utilizar servidores intermediarios o servicios tales como terminales Internet públicos, redes inalámbricas y servicios móviles de pago previo que no exigen autenticación. Las tecnologías de cifrado, que constituyen una solución técnica fundamental para garantizar la confidencialidad, integridad y disponibilidad de los datos, también pueden servir para ocultar identidades o al menos ralentizar el avance de las investigaciones sobre los orígenes de los ciberataques. Los procesos y políticas técnicos que limitan la retención de datos sobre el tráfico Internet también contribuyen a este problema de atribución y ubicación.

El riesgo de represalias contra un objetivo equivocado, así como las incertidumbres con respecto a los daños colaterales que puede causar un contraataque cibernético, que podría perjudicar fácilmente a un aliado o a un tercero inocente, frustraría aún más la capacidad de los Estados de responder a un ataque[188]. Si los agresores confían en que pueden pasar desapercibidos o piensan que sus víctimas no responderán con medios militares por temor a apartarse de las normas internacionales, las amenazas de represalias tienen muy poca influencia. Si se responde con la fuerza a un ataque cibernético que no ha recurrido a medios militares convencionales y tenía por objeto el aprovechamiento más que la destrucción, las represalias pueden ser interpretadas

---

186 Radical Change (quoting former U.S. security advisor Richard Clarke as stating that, "the force that prevented nuclear war – deterrence – does not work well in cyberwar").

187 Tang Lan y Zhang Xin, "Can Cyber Deterrence Work?" en Global Cyber Deterrence: Views from China, The U.S., Russia, India, and Norway, EastWest Institute, abr. 2010, p. 1, www.ewi.info/system/files/CyberDeterrenceWeb.pdf.

188 James A Lewis, "Cross-Domain Deterrence and Credible Threats", Center for Strategic and International Studies, jul. 2010, http://csis.org/files/publication/100701_Cross_Domain_Deterrence.pdf.

por la comunidad internacional como una agresión injustificada[189]. La estrategia de la disuasión también incita a los países a adoptar actitudes amenazadoras y a inventar diversas nuevas amenazas disuasivas para compensar posibles desequilibrios, lo que suprime las ventajas de la integración y aumenta las tensiones entre los países[190]. En todos estos casos, las características fundamentales del ciberespacio socavan la eficacia de la disuasión para lograr la paz cibernética.

Es posible que los propios planteamientos jurídicos existentes ya no sean apropiados para gestionar los riesgos de la ciberseguridad. Por ejemplo, según la legislación internacional plasmada en el Artículo 51 de la Carta de las Naciones Unidas, un Estado puede ejercer legítimamente su derecho de legítima defensa si es objeto de un ataque armado. En el contexto de la ciberguerra se plantean por supuesto dudas adicionales sobre si un ataque cibernético se puede considerar equivalente a un ataque armado y, en ese caso, si el ataque se puede atribuir a un Estado-nación[191]. La doctrina establecida de "responsabilidad del Estado" parece arrojar cierta luz sobre esta última cuestión. Consiste en que cada Estado debe actuar para impedir que su territorio se utilice para realizar ataques contra otros Estados y, si se niega a tomar medidas preventivas, puede ser considerado responsable de esos ataques. Ahora bien, como hemos observado en nuestras evaluaciones preliminares de los ciberataques, es sumamente difícil contestar a este tipo de preguntas prácticas en el ciberespacio, ya que algunos ataques no tienen origen geográfico (como ocurre con las "redes robot"), pueden saltar varias fronteras, tener su origen en coaliciones ubicadas en varias jurisdicciones o ser transmitidas por representantes que sólo actúan en nombre del auténtico autor. En algunos casos los propios Estados pueden ser incapaces de detectar o comprobar quién actúa en su propio territorio y, aunque puedan identificarlo, las características específicas del mundo cibernético impiden que una sola entidad pueda ejercer un control completo[192]. Así pues, es inevitable que la cuestión del origen y también del control se vuelva muy opaca.

b) Necesidad de un marco internacional

Habida cuenta de que las normas y los instrumentos jurídicos actuales no son suficientes para afrontar los nuevos problemas de la ciberseguridad, se necesitan ahora debates y métodos de colaboración internacionales. El carácter cambiante de la

---

189 Id.

190 Id.

191 Workshop p. 14.

192 Id.

propia tecnología, que da lugar a solapamientos crecientes entre las jurisdicciones nacionales y sus TIC, recursos y sistemas en línea, implica que es aún más importante adoptar nuevas estrategias y fomentar la cooperación internacional para garantizar la paz cibernética193.

Los ciberataques pueden originarse y golpear en cualquier lugar del mundo, por lo que esas amenazas son inherentemente internacionales y exigen una cooperación internacional, investigaciones comunes y disposiciones sustantivas y de procedimiento comunes para tratarlas de manera adecuada. Además, ya se reconoce por lo general que la cooperación internacional es una de las exigencias fundamentales para garantizar la ciberseguridad mundial. En 2003 y 2005, los países participantes en la Cumbre Mundial sobre la Sociedad de la Información (CMSI) convinieron en que se necesitaban instrumentos nacionales e internacionales eficaces para promover la cooperación internacional en materia de ciberseguridad[194]. Esta colaboración internacional debería estar motivada por un deseo común de paz, y también por el interés personal cabal de cada país. Todos los países dependen ahora de la tecnología para el comercio, las finanzas, la atención sanitaria, los servicios de emergencia, la distribución de alimentos y mucho más. La deterioración de redes vitales incapacitaría a cualquier país, y ninguno es inmune a los ciberataques. La preeminencia de las TIC y el hecho de que muchas de las nuevas tecnologías dependen unas de otras están dando lugar a un nuevo orden mundial en el que es necesario colaborar sobre las nuevas problemáticas para garantizar la estabilidad.

Es fundamental que los países armonicen sus marcos legislativos para luchar contra la ciberdelincuencia y facilitar una cooperación internacional dinámica y polifacética. Los Estados deberían colaborar para crear un marco legislativo y normativo común y establecer un sistema para actualizar periódicamente esas legislaciones a fin de tener en cuenta el carácter cambiante de las amenazas contra la seguridad. Varios grupos ya han pedido que se promulguen normas internacionales y normas sobre la informática para mejorar la ciberseguridad internacional[195]. En cualquier caso, una estrategia

---

193 Id.

194 "CMSI: Agenda de Túnez para la Sociedad de la Información", § 40, Cumbre Mundial sobre la Sociedad de la Información , WSIS-05/TUNIS/DOC/6(Rev.1)-E, 18 nov. 2005, www.itu.int/wsis/docs2/tunis/off/6rev1.html (en adelante "Agenda de Túnez").

195 Los participantes en un taller, que comprendían miembros del American Bar Association Standing Committee on Law and National Security, la McCormick Foundation y el National Strategy Forum contemplaron la creación de un Grupo especial sobre ciberseguridad internacional encargado de concebir normas y reglas para mejorar la ciberseguridad. Workshop p. 26.

eficaz destinada a lograr la paz cibernética debe ser suficientemente flexible y adaptable para tener en cuenta la rapidez de los cambios tecnológicos, el crecimiento de las TIC y los correspondientes problemas de seguridad, y responder a ellos. Los países también deben convenir en procedimientos y planteamientos para seguir el rastro de los orígenes e identidades a fin de encarar los ciberataques anónimos y las dificultades internacionales que éstos pueden crear. Las propuestas de un acuerdo internacional que exigiría que todos los países vigilaran su propio ciberespacio tratan de solucionar el problema de la atribución. Vincular la responsabilidad con el origen geográfico podría obviar el complicado proceso de identificar exactamente quién ha organizado un ataque cibernético[196]. Con todo, estas propuestas no resuelven el problema de la identificación de los intermediarios y de la ubicación del ataque en un lugar geográfico, el lugar correcto. Dadas las deficiencias de los planteamientos tradicionales y actuales de la seguridad internacional, es evidente que la comunidad mundial debe adoptar una nueva estrategia para afrontar las dificultades de la ciberseguridad y garantizar un ciberespacio duradero.

7.4 Propuestas de principios internacionales en el ciberespacio

Cuando se promulgan principios orientadores del ciberespacio, deben tenerse en cuenta sus características y las principales dificultades que éstas plantean. Podemos inspirarnos, por ejemplo, de otras actividades destinadas a contrarrestar amenazas transnacionales similares, tales como la Convención contra la Delincuencia Organizada Transnacional. A semejanza del crimen organizado transnacional, los ciberataques desconocen las fronteras y se propagan por complejas redes que imitan o se superponen a sistemas pacíficos y productivos. La Convención ilustra la opinión común de que estos omnipresentes problemas internacionales se deben afrontar con una estrecha cooperación internacional y de que se han de adoptar nuevas normativas, crear nuevos sistemas de asistencia recíproca en materia de legislación y desarrollo y de divulgación de información, así como de cooperación jurídica[197].

Conocidos principios jurídicos y normas internacionales ya contienen ciertos elementos indispensables de un plan para el ciberespacio. En particular, en el

---

196 Robert Mullins, "'Pearl Harbor' post struck a nerve", NetworkWorld, 11 mar. 2010, www.networkworld.com/community/node/58450 (se cita a un antiguo asesor presidencial estadounidense sobre seguridad, Richard Clarke en un reciente panel sobre ciberseguridad).

197 Convención contra la Delincuencia Organizada Transnacional, Oficina de las Naciones Unidas contra la Droga y el Delito, 2004, www.unodc.org/unodc/en/treaties/CTOC/index.html.

Artículo 19 de la Declaración Universal de Derechos Humanos se estipula que todo individuo tiene derecho a la libertad de opinión y de expresión, y que este derecho incluye el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión[198]. En su Declaración de Principios de Ginebra de 2003, la Cumbre Mundial sobre la Sociedad de la Información (CMSI) reafirma la noción de que la libertad de comunicar es un fundamento esencial de la Sociedad de la Información[199]. En la Declaración se destaca asimismo que la comunicación es un proceso social fundamental, una necesidad humana básica y el fundamento de toda organización social. En consecuencia, todas las personas deben tener un acceso equitativo a las tecnologías de la información y la comunicación. Estados Unidos ha articulado su compromiso a fin de velar por que todos dispongamos de este acceso y podamos aprovechar plenamente el potencial de la revolución digital[200].

La tecnología nuclear y las TIC son muy diferentes, pero la colaboración para garantizar la paz nuclear puede servir de ejemplo a una estrategia para el ciberespacio. Como el ciberespacio y las TIC, la energía y la tecnología nucleares tienen diversos usos pacíficos y militares, pueden ocasionar daños devastadores si se utilizan con fines bélicos y, a pesar de que el ataque puede estar dirigido contra un solo país, muchos países pueden sufrir sus consecuencias[201]. La comunidad internacional reconoce que la amenaza de ataque nuclear es mundial y, por lo tanto, ha tratado de elaborar una estrategia de colaboración multilateral que entrañe la creación de un planteamiento y un compromiso comunes de la seguridad nuclear[202]. Los tratados como el de no proliferación de armas nucleares (TNP) son testimonio de la voluntad de preservar los usos pacíficos de materiales potencialmente asoladores que desconocen las fronteras nacionales. En el TNP se determinan las responsabilidades por esos materiales sobre la base de la jurisdicción territorial o de las actividades

---

198 Declaración Universal de los Derechos Humanos, Artículo 19, AGNU, Res. 217A (III), U.N. GAOR, U.N. Doc. A/810, 1948, www.un.org/en/documents/udhr/index.shtml#a19.

199 Declaración de Principios de Ginebra, § 4, Cumbre Mundial sobre la Sociedad de la Información, 2003,: www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf.

200 "Ban urges greater use of digital technology to improve living conditions", UN News Centre, 17 may. 2010, www.un.org/apps/news/story.asp?NewsID=34716.

201 Declaración Nacional de Estados Unidos, 2010 Cumbre de Seguridad Nuclear, 13 abr. 2010, www.whitehouse.gov/the-press-office/nuclear-security-summit-national-statement-united-states (en adelante "Declaración Nacional de Estados Unidos").

202 Id.

"efectuadas bajo [el] control [de un Estado] en cualquier lugar"[203]. Cuarenta y siete países se han hecho eco de este planteamiento y han renovado su compromiso de garantizar la seguridad del material nuclear que se encuentra bajo su control, seguir mejorando la seguridad en función de las condiciones e intercambiar prácticas idóneas y soluciones prácticas en materia de seguridad en la Cumbre de Seguridad Nuclear de 2010[204].

En el TNP se insiste asimismo en las ventajas de las aplicaciones pacíficas de la tecnología nuclear y en la importancia de que todos los países, incluidos los países en desarrollo, puedan aprovechar sus ventajas[205]. En el tratado se insiste en la importancia de la cooperación internacional entre todos los Estados y, en particular, el intercambio de información y de material para contribuir al desarrollo de aplicaciones pacíficas de la energía atómica[206]. Además, el Artículo 3 del TNP obliga a los signatarios a adoptar ciertas medidas destinadas a impedir que la energía nuclear no se utilice para fines pacíficos y sirva para la fabricación de armas nucleares u otros fines de destrucción[207]. La Agencia Internacional de Energía Atómica, organismo reconocido por su experiencia, conocimientos y capacidad para facilitar los debates en un foro neutro, está encargada de supervisar la negociación y concertación de un acuerdo entre los Estados en el que se establecerá un sistema de protección de ese tipo[208]. Otras colaboraciones internacionales tienen por objeto garantizar la paz nuclear, tales como la Iniciativa Mundial para Combatir el Terrorismo Nuclear, una asociación internacional de países que se han comprometido a trabajar individual y colectivamente para aplicar una serie de principios de seguridad nuclear[209]. Estos principios consisten, entre otras cosas, en la elaboración y el perfeccionamiento de medidas de responsabilidad, control y seguridad en lo que respecta a las sustancias nucleares y las instalaciones nucleares civiles, el mejoramiento de las capacidades de detección y control de los estados miembros, la prevención de la creación de refugios

---

203 Tratado sobre la no proliferación de armas nucleares, Art. 3, 1970, www.un.org/disarmament/WMD/Nuclear de 1000/pdf/NPTEnglish_Text.pdf (en adelante "TNP").

204 Declaración Nacional de Estados Unidos.

205 TNP en preámbulo y Art. 5.

206 Id. p. Preámbulo.

207 Id. en Art. 3.

208 Id.

209 "The Global Initiative to Combat Nuclear Terrorism", Departamento de Estado de EE.UU., www.state.gov/t/isn/c18406.htm.

para los terroristas, el mejoramiento de las capacidades de respuesta, mitigación e investigación de los miembros en caso de ataque y la promoción de la divulgación de información[210].

Los esfuerzos internacionales encaminados a garantizar la paz en nuevos ámbitos aparentemente ilimitados también promueven fuertemente una amplia cooperación internacional. Por ejemplo, entre otros principios orientadores, en la Declaración de los Principios Jurídicos que Deben Regir las Actividades de los Estados en la Exploración y Utilización del Espacio Ultraterrestre se propone que en la exploración y la utilización del espacio ultraterrestre todos los Estados se guíen por el principio de la cooperación y la asistencia mutua[211].

Habida cuenta de que el riesgo de ciberataques colectivos de todo tipo no deja de aumentar, el Secretario General de la UIT propone cinco principios orientadores para establecer y mantener la paz en el nuevo mundo cibernético. Estos principios encarnan y promueven los valores y la cultura de la Unión Internacional de Telecomunicaciones, que se han ilustrado durante su largo historial dirigiendo la normalización y la reglamentación internacional. El Reglamento de las Telecomunicaciones Internacionales (RTI) de la UIT es uno de los numerosos ejemplos de esta tradición de promover el desarrollo armonioso, la explotación eficaz y el acceso universal a las telecomunicaciones internacionales y la tecnología. La elaboración del RTI tenía por objeto determinar un nuevo marco normativo para tratar las nuevas cuestiones y dificultades que planteaba el nuevo mundo de las telecomunicaciones que se materializó a finales de los años 80[212]. Se redactaron para promover la eficacia y el desarrollo en un contexto de colaboración, cooperación y acceso equitativo, otro ejemplo más de la tradición de la UIT. También reflejan la voluntad de la organización de proteger el derecho a comunicar y proteger las instalaciones.

---

210 "Statement of Principles", The Global Initiative to Combat Nuclear Terrorism, Departamento de Estado de EE.UU., www.state.gov/documents/organization/141995.pdf.

211 Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space (the "Outer Space Treaty"), Principle 6, 1967, www.oosa.unvienna.org/oosa/SpaceLaw/lpos.html.

212 "Reglamento de las Telecomunicaciones Internacionales: Actas Finales de la Conferencia Administrativa Mundial Telegráfica y Telefónica", Unión Internacional de Telecomunicaciones, 1989, www.itu.int/osg/spu/intset/itu-t/mel88/mel-88-e.pdf.

Los cinco principios siguientes definidos por el Secretario General de la UIT para el ciberespacio comprenden también estos valores esenciales y establecen acciones y obligaciones específicas que garantizarán la paz y estabilidad en el ciberespacio:

1. Los gobiernos deben comprometerse a dar acceso a todos los ciudadanos a las comunicaciones.
2. Los gobiernos deben comprometerse a proteger a sus ciudadanos en el ciberespacio.
3. Los países deben comprometerse a no dar refugio a terroristas/delincuentes en su territorio.
4. Los países deben comprometerse a no lanzar el primer ataque cibernético contra otros países.
5. Los países deben comprometerse a colaborar en un marco de cooperación internacional para garantizar la paz en el ciberespacio.

8 Agenda de la UIT sobre ciberseguridad global

Por Hamadoun I. Touré

La UIT es un foro mundial único para debatir cuestiones de ciberseguridad. Desde su fundación en 1865 hace casi 145 años, la organización ha desempeñado diversos papeles importantes en las telecomunicaciones, la seguridad de la información y la normalización. La UIT es consciente de que la escala y la naturaleza del problema de la ciberseguridad exigen una acción colectiva coordinada y, en consecuencia, trabaja para alcanzar ese objetivo. En particular, promueve actualmente la ciberseguridad por conducto de diversas actividades relacionadas con la normalización y la asistencia técnica adaptadas a las necesidades específicas de los países en desarrollo. Los dirigentes y gobiernos de todo el mundo reconocen la dilatada experiencia, la capacidad y los conocimientos de la UIT, y la han nombrado facilitador único de la Línea de Acción C5 de la CMSI, "Creación de confianza y seguridad en la utilización de las TIC"[213]. Por este motivo, Jefes de Estado y otros dirigentes mundiales que participaban en la CMSI, así como Estados Miembros de la UIT, encomendaron a la organización que abriera camino adoptando medidas concretas para poner freno a las amenazas e inseguridades relacionadas con la Sociedad de la Información. En su Resolución 140 (Rev. Antalya 2006), la Conferencia de Plenipotenciarios de la UIT aborda la función de la UIT en la puesta en práctica de los resultados de la CMSI y encarga al Secretario General que tome las medidas necesarias para que la UIT pueda asumir sus funciones.

En cumplimiento de ese mandato, el Secretario General lanzó en mayo de 2007 la Agenda sobre ciberseguridad global (ACG) con objeto de crear un marco en el que todos los interesados puedan coordinar una respuesta internacional al creciente problema de la ciberseguridad. La ACG se fundamenta en la cooperación internacional y se esfuerza por que todos los interesados se concierten para crear confianza y seguridad en la sociedad de la información. Hace poco tiempo los Estados Miembros confirmaron la labor de la UIT en este campo en la Conferencia de Plenipotenciarios de 2010 y confirmaron que la ACG es el marco de cooperación internacional en la Resolución 130 (Rev. Guadalajara, 2010), en la que se encarga al Secretario General que siga examinando y mejorando los avances realizados en el marco de sus funciones. Los Estados Miembros observan en particular el fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las TIC, así como

---

213 Agenda de Túnez.

la iniciativa mundial de la Unión en colaboración con la Alianza Internacional Multilateral contra las Ciberamenazas (IMPACT) y el Foro de los equipos de respuesta en caso de incidentes de seguridad (FIRST). También se resuelve atribuir una gran prioridad en la UIT a sus trabajos sobre la seguridad de las redes de información y comunicación.

La ACG tiene por objeto alcanzar las siete metas estratégicas siguientes:

a) Preparar estrategias que promuevan el desarrollo de una legislación modelo sobre ciberdelito, que resulte aplicable a escala mundial y sea compatible con las medidas legislativas ya adoptadas en los diferentes países y regiones.

b) Definir estrategias mundiales para crear las adecuadas estructuras institucionales nacionales y regionales, así como definir las correspondientes políticas para luchar contra el ciberdelito.

c) Diseñar una estrategia que permita establecer un conjunto mínimo y mundialmente aceptado de criterios de seguridad y planes de acreditación para equipos, aplicaciones y sistemas informáticos.

d) Definir estrategias para crear un marco mundial con miras a vigilar, alertar y responder ante incidentes y garantizar así la coordinación transfronteriza en lo que concierne a las iniciativas nuevas y existentes.

e) Diseñar estrategias mundiales tendentes a crear y apoyar un sistema de identidad digital genérico y universal y las correspondientes estructuras institucionales para garantizar el reconocimiento internacional de credenciales digitales.

f) Concebir una estrategia global para facilitar la creación de capacidad humana institucional con el fin de promover los conocimientos técnicos y prácticos en todos los sectores y las esferas antes mencionadas.

g) Formular propuestas para establecer un marco conducente a una estrategia mundial multipartita que fomente la cooperación, el diálogo y la coordinación internacionales en todas las esferas precitadas.

Para alcanzar esas metas, la ACG se basa en los cinco pilares siguientes a fin de orientar sus sectores de actividad:

1. Medidas legales

La ciberdelincuencia organizada aumenta porque Internet es lucrativo y poco arriesgado, debido a las lagunas que persisten en las legislaciones nacionales y regionales que incluso dificultan la persecución eficaz de los delincuentes. En la estructura de la ACG, este pilar tiene por objeto elaborar estrategias para desarrollar

legislaciones modelo sobre la ciberdelincuencia aplicables y compatibles a escala mundial. Mediante sus diversos recursos en materia de legislación de la ciberdelincuencia, la UIT ayuda a los Estados Miembros a comprender los aspectos jurídicos de la ciberseguridad a fin de que puedan armonizar sus marcos legislativos.

2. Medidas técnicas y de procedimientos

Este pilar se centra en las medidas destinadas a tratar las vulnerabilidades de los productos informáticos, con objeto de concebir sistemas, protocolos y normas de acreditación aceptables a escala mundial. La UIT y, en particular, sus Sectores de Normalización (UIT-T) y de Radiocomunicaciones (UIT-R), se encuentran en una posición ideal en el mundo de la normalización de las TIC y también desempeñan un papel vital en el estudio de las vulnerabilidades de seguridad de los protocolos. Con miras a identificar ciberamenazas y medidas para limitar los riesgos, la UIT está estudiando mejoras de los servicios de comunicación seguros para perfeccionar las especificaciones de seguridad de las comunicaciones de datos móviles de extremo a extremo y estudia los requisitos de seguridad de los protocolos de servicios y aplicaciones web. Los Grupos Temáticos y Comisiones de Estudio de la UIT, tales como el recientemente creado Grupo Temático sobre las redes eléctricas inteligentes, son mecanismos eficaces para alcanzar esas metas.

3. Estructuras institucionales

Todos sabemos por experiencia que los sistemas de vigilancia y alerta y la respuesta a incidentes son esenciales para responder a los ciberataques, como lo es la libre circulación de información, la colaboración y la cooperación en las estructuras orgánicas nacionales y entre ellas. Este pilar, por consiguiente, tiene la finalidad de crear estructuras y estrategias orgánicas para ayudar a impedir, detectar y responder a ataques contra infraestructuras esenciales de la información. A este respecto, la UIT está colaborando con los Estados Miembros para tratar de identificar sus necesidades concretas en materia de ciberseguridad y ayudarlos a establecer equipos encargados de los incidentes informáticos (CIRT). Por otra parte, en el marco de la colaboración de la UIT con la Alianza Internacional Multilateral contra las Ciberamenazas (IMPACT), el Centro de Respuesta Global (CRG) desempeña un papel fundamental en la consecución de los objetivos de la ACG.

La UIT e IMPACT firmaron oficialmente un Memorándum de Entendimiento por conducto del cual la modernísima sede de IMPACT en el Cyberjaya (Malasia) se ha convertido de hecho en la sede física de la ACG. Gracias a esta colaboración, los 192 Estados Miembros de la UIT disponen de los conocimientos, instalaciones y recursos

necesarios para afrontar las ciberamenazas más graves del mundo. Dadas las estrechas sinergias entre los dos ámbitos de trabajo de la ACG y los servicios e infraestructuras proporcionados por IMPACT, esta asociación es una etapa lógica en la lucha mundial contra las ciberamenazas. Unos 60 países ya se han adherido a esta colaboración[214].

IMPACT proporciona recursos de respuesta de emergencia para facilitar la identificación de ciberamenazas y compartirán recursos para ayudar a los Estados Miembros[215]. El Centro de Respuesta Global (CRG) está equipado con una sala de crisis, modernísimos equipos informáticos y de comunicaciones, un centro de operaciones de seguridad totalmente funcional y siempre activo, un centro seguro de datos totalmente redundante, instalaciones para los trabajadores que hacen turnos, un centro de radiodifusión propio y una galería de visitas para personalidades. El CRG desempeña pues un papel fundamental en la consecución del objetivo de la ACG de adoptar medidas técnicas para luchar contra las nuevas ciberamenazas y la evolución de las mismas. Los dos elementos más destacados del CRG son NEWS (sistema de alerta temprana en red) y ESCAPE (plataforma de aplicación de colaboración electrónicamente segura para expertos). El programa NEWS ayuda a los países miembros a identificar rápidamente ciberamenazas y proporciona información esencial sobre las medidas que sean adoptadas para mitigarlas. El programa ESCAPE es uno de los instrumentos y sistemas especializados de que dispondrán los Estados Miembros. Se trata de un sistema electrónico con el que ciberexpertos autorizados de varios países pueden unir recursos y colaborar a distancia en un entorno seguro y fiable. ESCAPE permite reunir rápidamente recursos y conocimientos de muchos países diferentes y, de este modo, los países, individual y colectivamente, pueden responder inmediatamente a ciberamenazas, especialmente en situaciones de crisis.

Los objetivos y recursos de esta colaboración corresponden a los cinco pilares de la ACG, y también corresponden estrechamente a los principios propuestos para la ciberpaz. Los recursos de que disponen los Estados Miembros a través de IMPACT ayudarán a los gobiernos a proteger a sus ciudadanos contra ciberataques y garantizar así un acceso permanente a las comunicaciones a través de Internet y otras TIC. Cuando se adhieren a IMPACT y participan en la compartición de recursos y los

---

214 "International Multilateral Partnership Against Cyber Threats", Unión Internacional de Telecomunicaciones, www.itu.int/ITU-D/cyb/cybersecurity/impact.html.

215 Carta de información de la UIT enviada a todos los Estados Miembros de la UIT sobre "Deployment of Cybersecurity Capabilities - IMPACT Global Response Centre", www.itu.int/ITU-D/cyb/cybersecurity/docs/IMPACT-information-letter-sent-to-member-states-2009.pdf.

debates con otros Estados Miembros, los Estados también persiguen activamente el quinto principio, el compromiso de colaborar en un marco internacional para garantizar la ciberpaz. Además, IMPACT también ofrece a los Estados Miembros en desarrollo que reúnen las condiciones, becas para cursos de capacitación que tendrá por objeto crear un acervo de recursos y adquirir conocimientos que los alumnos podrán compartir después con otros para crear capacidades y conocimientos nacionales en materia de ciberseguridad. Esas becas mejorarán las capacidades de los países para a obtener sus propios recursos TIC y también garantizar el acceso de sus propios ciudadanos.

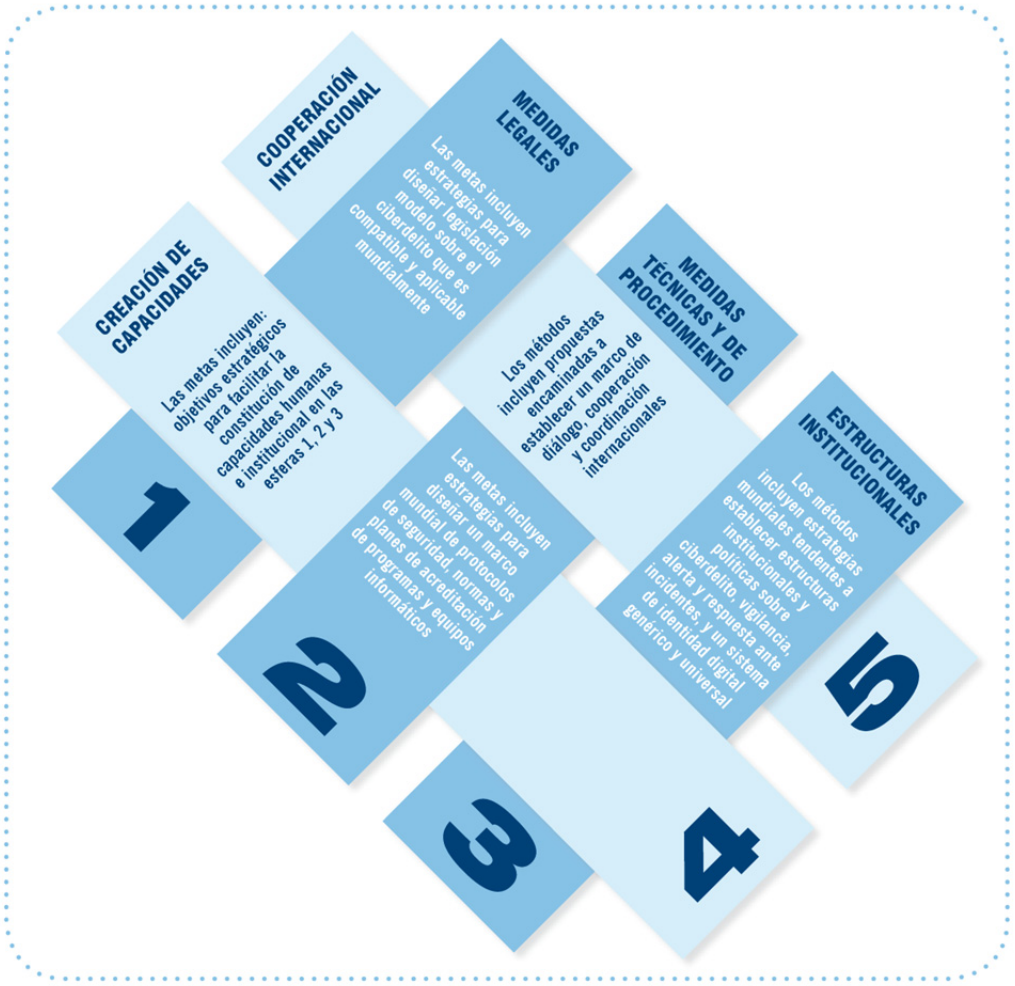
4. Creación de capacidades

En el marco de la ACG, este pilar tiene por objeto elaborar estrategias para mejorar los conocimientos y capacidades a fin de aumentar la importancia de la ciberseguridad en las agendas de políticas nacionales. Se debe promover la creación de capacidades para desarrollar una cultura sostenible y dinámica de la ciberseguridad. Es esencial comprender y divulgar los peligros potenciales del ciberespacio para que los usuarios puedan beneficiarse de las TIC con seguridad. En particular, en cumplimiento de su mandato de ayudar a los Estados Miembros a desarrollar capacidades de ciberseguridad, la UIT procura facilitar la implementación y el despliegue de capacidades de ciberseguridad con publicaciones tales como su Guía sobre Ciberseguridad Nacional, sus Recursos sobre el ciberdelito y el Conjunto de herramientas para la mitigación de redes robot.

5. Cooperación internacional

La ciberseguridad es tan internacional y trascendental como Internet. Por consiguiente, los cinco pilares de la ACG se refieren a estrategias de cooperación, diálogo y coordinación internacionales. La colaboración IMPACT es un progreso considerable en este sentido, ya que ofrece a los Estados Miembros y a terceros una plataforma para estudiar políticas y compartir información, y promueve directamente el mandato encomendado a la UIT por numerosos Estados Miembros en el marco de la Línea de Acción C5 de la CMSI. En la Declaración de Principios de la CMSI se indica que el fomento de un clima de confianza, incluso en la seguridad de la información y la seguridad de las redes, la autenticación, la privacidad y la protección de los consumidores, es requisito previo para que se desarrolle la Sociedad de la Información y para promover la confianza entre los usuarios de las TIC. Para ello se debe fomentar, desarrollar y poner en práctica una cultura global de ciberseguridad, en cooperación con todas las partes interesadas y los organismos internacionales especializados. El sistema de colaboración IMPACT, al que se suman los Grupos Temáticos y el RTI,

refuerza este marco de confianza, facilita la obtención de estas metas gracias a un planteamiento exhaustivo y ofrece un lugar de reunión a todos los miembros de la comunidad mundial.



Agenda sobre ciberseguridad global: Cinco pilares

Conclusión

Si bien las amenazas que acompañan al desarrollo cibernético y la creciente dependencia de las TIC son preocupantes, sus posibles ventajas las compensan con creces. Algunos de los riesgos de la ciberguerra ya se han materializado, pero también hemos cosechado ya los frutos del ciberespacio, y las promesas de futuras cosechas son infinitas. A medida que avanzamos, debemos determinar claramente cómo seguir aumentando la dependencia, el desarrollo y la integración cibernéticos, cómo proteger los recursos, crear un entorno estable para que sigan prosperando las infraestructuras y las nuevas tecnologías, y garantizar una paz duradera. Muchas de las propuestas actuales son positivas, pero son insuficientes y quizá no sean la solución más eficaz. También es muy posible que trabajando juntos podamos alcanzar estos objetivos y evitar las funestas consecuencias de un ciberconflicto. La UIT ya lleva a cabo diversas actividades encaminadas a alcanzar este objetivo y disponer de los recursos y la influencia necesarios para obtener el apoyo y la participación multilaterales requeridos.

9 Declaración de Erice sobre Principios de Estabilidad y Paz Cibernéticas

Por Federación Mundial de Científicos

Declaración de Erice sobre Principios de Estabilidad y Paz Cibernéticas

Es un *triunfo sin precedente de la ciencia* que la humanidad, mediante la utilización de modernas tecnologías de la información y la comunicación (TIC), disponga ahora de los medios necesarios para aumentar los recursos económicos de todos los países, mejorar las capacidades intelectuales de sus ciudadanos, y desarrollar su cultura y su confianza en otras sociedades. Internet, como la propia ciencia, es fundamentalmente transnacional y ubicua. Internet, y sus correspondientes instrumentos de información, es el conducto indispensable por el que los científicos disertan a escala nacional e internacional y ofrecen a todos los beneficios de una ciencia libre sin secretos ni fronteras.

En el siglo XXI, Internet y las demás redes interconectadas (ciberespacio) se han vuelto indispensables para el bienestar de la especie humana, la independencia política y la integridad territorial de los países.

El peligro estriba en que el mundo está tan interconectado y los riesgos y amenazas son tan sofisticados y omnipresentes que han crecido exponencialmente en comparación con la capacidad de contrarrestarlos. Los países, y también los delincuentes, disponen ahora de la capacidad para perturbar considerablemente la vida y la sociedad de todos los países; la ciberdelincuencia y su vástago, el ciberconflicto, amenazan la paz de la humanidad y la utilización beneficiosa del ciberespacio.

Los sistemas y redes de información y comunicación sustentan la seguridad nacional y económica de todos los países y sirven de sistema nervioso central para las capacidades de respuesta, las operaciones comerciales y gubernamentales, los servicios públicos, la salud pública y el enriquecimiento personal.

Los sistemas e infraestructuras de la información se están volviendo indispensables para la salud, la seguridad y el bienestar de las personas y, especialmente, los ancianos, discapacitados, enfermos y muy jóvenes. Las grandes perturbaciones del ciberespacio pueden causar sufrimientos y destrucciones innecesarios.

Las TIC apoyan los principios de los derechos humanos garantizados por la legislación internacional, como por ejemplo la *Declaración Universal de Derechos Humanos*

(Artículos 12, 18 y 19) y el *Pacto Internacional de Derechos Civiles y Políticos* (Artículos 17, 18, y 19). Las perturbaciones del ciberespacio: a) perjudican el derecho de los individuos al respeto de la vida privada, la familia, el domicilio y la correspondencia sin interferencias ni ataques, b) interfieren con el derecho a la libertad de pensamiento, de conciencia y de religión, c) limitan el derecho a la libertad de opinión y de expresión, y d) limitan el derecho a recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión.

Las TIC pueden ser beneficiosas o perjudiciales y, por lo tanto, también pueden ser un instrumento de paz o de conflicto. Para cosechar los beneficios de la era de la información los sistemas y redes de información deben ser estables y fiables, estar disponibles y ser dignos de confianza. Garantizar la integridad, seguridad y estabilidad del ciberespacio en general exige una acción internacional concertada.

POR CONSIGUIENTE, recomendamos los siguientes principios para lograr y mantener la estabilidad y la paz cibernéticas:

1. Todos los gobiernos deberían reconocer que la legislación internacional garantiza la libre circulación de información e ideas; esas garantías también se aplican al ciberespacio. Sólo se deberían aplicar restricciones en caso de necesidad, y éstas deberían ir acompañadas de un proceso legislativo.
2. Todos los países deberían colaborar para elaborar un código común de conducta y un marco legislativo mundial armonizado que comprendiera disposiciones de procedimiento relativas a la asistencia y cooperación en las investigaciones que respeten la privacidad y los derechos humanos. Todos los gobiernos, proveedores de servicios y usuarios deberían apoyar los esfuerzos de aplicación de la legislación internacional contra los ciberdelincuentes.
3. Todos los usuarios, proveedores de servicios y gobiernos deberían colaborar para velar por que la utilización del ciberespacio no entrañe la explotación de los usuarios, en particular los jóvenes y las personas sin defensa, por medios violentos o degradantes.
4. Los gobiernos como las organizaciones del sector privado, incluidas las personas físicas, deben de aplicar y mantener programas de seguridad integrales basados en prácticas idóneas y normas universalmente aceptadas que recurran a tecnologías de privacidad y seguridad.
5. Los desarrolladores sean de programación y equipos informáticos deberían tratar de desarrollar tecnologías seguras que promuevan la capacidad de recuperación y resistan a las vulnerabilidades.

6. Los gobiernos deberían participar activamente en los esfuerzos de las Naciones Unidas encaminados a promover la seguridad y la paz cibernética mundiales y evitar la utilización del ciberespacio para fines bélicos.

La Declaración de Erice sobre Principios de Estabilidad y Paz Cibernéticas fue redactada por el Panel permanente de supervisión de la seguridad de la información de la Federación Mundial de Científicos (WFS), Ginebra, y adoptada por el Pleno de la WFS con ocasión de la 42ª reunión de los Seminarios Internacionales sobre Emergencias Planetarias en Erice (Sicilia) el 20 de agosto de 2009.

10 Conclusión

Por Jody R. Westby

La lucha por el ciberespacio está sorprendentemente tranquila estos días. El Panel permanente de supervisión (PMP, *Permanent Monitoring Panel*) de la seguridad de la información de la Federación Mundial de Científicos (WFS, *World Federation of Scientists*) propuso por primera vez el concepto de ciberespacio en un programa fundador que presentó en la Academia Pontificia de Ciencias del Vaticano en diciembre de 2008. Posteriormente, el PMP redactó la "Declaración de Erice sobre Principios de Estabilidad y Paz Cibernéticas" en 2009, que fue adoptada por la WFS y distribuida a todos los miembros de las Naciones Unidas. Los conceptos y principios plasmados en esa publicación reflejan la preocupante opinión del PMP de que el mundo va derecho al caos informático, pero el trayecto hacia la ciberpaz generará una mayor estabilidad mundial.

Las estadísticas e hipótesis presentadas indican que es muy importante frenar la ciberdelincuencia e impedir los conflictos cibernéticos. Internet ha creado el crimen perfecto porque es difícil encontrar al culpable y pocas veces se le captura y juzga. Tememos que Internet también se esté convirtiendo en el arma ideal. Es muy fácil acceder a los datos más confidenciales de un país y a sus infraestructuras esenciales, y un país pequeño puede atacar a países con presupuestos de defensa muy superiores. Los países en desarrollo han mostrado a los países desarrollados como crear infraestructuras TIC de manera no lineal utilizando tecnologías de satélite e inalámbricas. Otros países están descubriendo que las proezas cibernéticas son una opción no lineal atractiva para defender los intereses de seguridad nacionales y económicos.

¿Por qué no se han puesto de moda la limitación o la paz cibernéticas? Los dirigentes militares de todo el mundo anuncian en cambio la creación de mandos informáticos y revelan sus planes de desarrollar capacidades de ataque, defensa y explotación de redes. Cuando los países se encontraron frente a armas nucleares, pidieron a gritos la limitación y la no proliferación. Los países hicieron causa común en todo el mundo para detener un peligro colectivo que amenazaba a la humanidad. Como demostraron los ataques contra Estonia y Georgia, cuando un país atacado se encuentra frente a un marco legislativo internacional deficiente, incertidumbres diplomáticas y limitaciones técnicas, y es incapaz de controlar sus comunicaciones, la noción de ciberpaz se vuelve atractiva.

Muchas organizaciones multinacionales estudian diversos aspectos de la ciberdelincuencia y/o los ciberconflictos, pero la UIT es la única que ha adoptado una

visión global y ha definido una agenda destinada a abordar los principales problemas aprovechando al mismo tiempo los esfuerzos de otras organizaciones. Debemos felicitar al Secretario General por su liderazgo, visión y valor a la hora de afrontar de cara tamaño problema. Esperamos sinceramente que otras organizaciones refrenden y emulen esa actitud y que los dirigentes decidan elaborar un código de conducta cibernético y un marco legislativo que propicie y fomente la estabilidad geocibernética.

Nos estamos acercando a un peligroso precipicio en el que el lado oscuro de Internet podría eclipsar las ingentes ventajas de las TIC y perturbar el orden mundial. Es hora de que llegue la ciberpaz.

Contacto:
División de Estrategia de la Unión
Unión Internacional de Telecomunicaciones
Place des Nations – 1211 Ginebra 20
Suiza
E-mail: strategy@itu.int
www.itu.int/cybersecurity

Impreso en Suiza
Ginebra, enero de 2011