Naciones Unidas | Unión Interparlamentaria | Unión Internacional de Telecomunicaciones

Cuarto Foro Parlamentario sobre la Configuración de la Sociedad de la Información. El triple reto de la ciberseguridad: Información, ciudadanos e infraestructura

18-20 de mayo de 2011
Sala II – Centro de Conferencias de la OIT
Organización Internacional del Trabajo
Ginebra, Suiza

NOTA RECORDATORIA

Contexto

Durante los últimos años se ha producido un aumento espectacular de los casos de actividad delictiva relacionada con Internet. Las denuncias de violaciones de datos y de la privacidad, así como los ciberataques, se han convertido en una noticia habitual en los medios de comunicación. Debido a su rápida expansión, a su carácter abierto y a las escasas barreras de entrada, la red mundial se está convirtiendo rápidamente en el ámbito favorito de un sinfín de actividades malintencionadas, como el correo indeseado, la pornografía infantil, los timos financieros y el espionaje industrial. La delincuencia organizada se ha implantado firmemente en Internet. Para los ciberdelincuentes, los costos de oportunidad son muy reducidos y el rendimiento potencial muy elevado. Controlan vastas redes de computadoras infectadas con programas informáticos maliciosos (*botnets*), de los que sus dueños no tienen conocimiento y que pueden ser utilizados de forma anónima para robar datos de usuarios y atacar a nuevas y confiadas víctimas. Alquilan sus servicios en un pujante mercado negro en línea en el que se comercializan datos de tarjetas de crédito, información sobre cuentas bancarias, direcciones de correo electrónico y otros datos conseguidos ilegalmente. Según las informaciones, la industria electrónica en la sombra ha experimentado un crecimiento de dos dígitos en 2010[1]. Se calcula que la ciberdelincuencia cuesta a las empresas de todo el mundo alrededor de 750.000 millones de euros al año[2]. Si bien es difícil disponer de información exacta, las pérdidas globales para la sociedad pueden ser mayores, ya que a menudo las pérdidas financieras de los particulares no se denuncian debidamente.

Debido a los avances en telecomunicaciones de banda ancha y telefonía móvil, cada vez más usuarios acceden a Internet y realizan transacciones utilizando nuevos aparatos de tecnología móvil como los teléfonos inteligentes (*smartphones*) y las tabletas electrónicas. Son, en esencia, nuevas plataformas de computación cuyos elementos de

1 UPI.com: *Cybercrime 'industry' sees double-digit growth*, http://www.upi.com/Business_News/Security-Industry/2011/03/02/Cybercrime-industry-sees-double-digit-growth/UPI-66271299103546/
2 Europol: *Cybercrime as a business*: *The digital underground economy*, http://www.europol.europa.eu/index.asp?page=news&news=pr110106.htm

seguridad todavía no están suficientemente desarrollados, por lo que ofrecen a los ciberdelincuentes un campo abonado en el que acceder a información confidencial y realizar transacciones no autorizadas a expensas de sus legítimos usuarios. Al mismo tiempo, estos ciudadanos, queriéndolo o no, revelan una impresionante cantidad de información personal sobre sí mismos en su uso regular y sostenido de las redes sociales, dejando literalmente detrás de sí un rastro virtual, suerte de migas informáticas, que puede ser fácilmente seguido con fines ilícitos. Sin que a menudo sean conscientes de las consecuencias que ello tiene para su privacidad, los usuarios son inducidos a desvelar públicamente más y más información sobre sus vidas privadas, lo que da lugar a una reformulación del propio concepto de privacidad en la era de Internet. La recopilación de datos privados, como los hábitos de consulta en Internet, las compras en línea, el círculo social de amigos y los destinos geográficos frecuentados son la base de modelos empresariales que alimentan una industria en la red que genera miles de millones de dólares de beneficios. No es de extrañar que la creciente economía de Internet también atraiga la atención de los ciberdelincuentes.

A pesar de los contados casos, de muy elevado perfil y a los que se ha dado mucha publicidad, de ciberdelincuentes capturados, está claro que la falta de una política consensuada a nivel internacional sobre ciberseguridad menoscaba los esfuerzos de los gobiernos. Casos recientes[3] de redes de pornografía infantil desmanteladas ilustran el nivel de cooperación internacional requerida, en virtud de la cual diversos organismos encargados de hacer cumplir la ley participan en operaciones minuciosamente coordinadas para detener a los culpables y desbaratar sus actividades delictivas.

En este entorno complejo y en rápida evolución, los gobiernos luchan por mantenerse al tanto del rápido avance del uso ilícito de innovaciones tecnológicas, a fin de velar por la seguridad de sus ciudadanos y proteger la información confidencial y las infraestructuras. La naturaleza mundial de Internet y el carácter internacional de la ciberdelincuencia son especialmente problemáticos para los gobiernos, ya que los ciberdelincuentes pueden ubicarse en cualquier parte del mundo y a menudo colaboran entre sí en la red sin tener que verse en persona. Las leyes y normativas difieren de un país a otro, lo que permite a los ciberdelincuentes disfrutar de refugios seguros en países que no han promulgado legislaciones adecuadas[4].

Además, el proceso político relativo a la negociación de acuerdos internacionales y la promulgación de disposiciones coordinadas sobre ciberseguridad está resultando ser lento si se compara con la evolución tecnológica. Desde la aprobación en 2001 del Convenio sobre la Ciberdelincuencia[5], han hecho su aparición en el panorama tecnológico Facebook, Twitter, los teléfonos inteligentes y la computación en la nube (*cloud computing*), así como los *botnets* y los "ataques de *phishing*", abriendo nuevos y más complicados frentes de debate.

Por otra parte, los gobiernos, a los que sus electorados presionan para que aborden las cuestiones que plantea la ciberseguridad, a menudo corren el riesgo de excederse en su reacción y de perturbar el delicado equilibrio existente entre las inquietudes de seguridad y los derechos fundamentales de los ciudadanos, un equilibrio que puede verse alterado por decisiones, voluntarias o involuntarias, del ejecutivo. Un estudio publicado por el Parlamento Europeo confirma que las TIC ofrecen nuevas oportunidades para proteger y promover los derechos humanos, pero que, al mismo tiempo, representan

3 V3.co.uk: *Hacker arrested on Mariposa botnet charges*, http://www.v3.co.uk/v3-uk/news/1950312/hacker-arrested mariposa-botnet-charges SV Mercury News: *International child porn ring is broken up*, http://www.mercurynews.com/california/ci_16857738

4 Por ejemplo, los recientes intentos de impedir el acceso a materiales confidenciales desvelados por Wikileaks resultaron en gran parte ineficaces ya que el contenido fue reproducido a través de cientos de servidores que quedan fuera del ámbito de aplicación de los acuerdos internacionales o bilaterales.

5 En 2001, el Consejo de Europa aprobó el Convenio sobre la Ciberdelincuencia, que entró en vigor en 2004. Cabe señalar que el Convenio no cuenta con un apoyo unánime.

amenazas directas para esos mismos derechos, ya que permiten el desarrollo de mecanismos de censura y de control cada vez más sofisticados[6].

En este contexto, es evidente que la ciberseguridad se ha convertido en una prioridad en la agenda de muchos gobiernos y de la comunidad internacional, ya que las consecuencias de las amenazas en la red son omnipresentes y exigen respuestas a nivel tanto nacional como internacional.

Por ser la institución pública que debe rendir cuentas en primer lugar ante el electorado sobre cómo garantizar la seguridad de los ciudadanos, preservar sus derechos y promover una sociedad de información centrada en las personas, los parlamentos tienen la especial responsabilidad de participar activamente en la tarea de orientar la agenda sobre ciberseguridad. Dado que los legisladores deben velar por que las leyes beneficien verdaderamente a los electorados que representan, corresponde a los parlamentarios tratar de lograr un equilibrio más razonable entre las diversas necesidades enfrentadas, promoviendo una sociedad de la información que reafirme y refuerce los derechos humanos fundamentales al tiempo que garantiza la seguridad de los ciudadanos y la protección de la información y las infraestructuras. Para ello, el parlamento debe ejercer plenamente su función de control sobre el ejecutivo y los organismos encargados de hacer cumplir la ley, examinando cuidadosamente cuáles han sido sus respuestas a las amenazas y desafíos de base tecnológica.

A nivel internacional, es mucho lo que los parlamentos pueden hacer para promover la coordinación y armonización mundiales de las leyes y normativas sobre ciberseguridad, mediante una cooperación y un intercambio crecientes entre los miembros de los parlamentos y las comisiones que se ocupan de esta cuestión.

Objetivos del Foro Parlamentario

El Foro Parlamentario "El triple reto de la ciberseguridad: Información, ciudadanos e infraestructura" es la cuarta reunión de miembros de parlamentos centrada en cuestiones relativas a la sociedad de la información organizada en el marco del Centro Mundial de las TIC en el Parlamento, iniciativa de cooperación puesta en marcha por el Departamento de Asuntos Económicos y Sociales (DAES) de las Naciones Unidas y la Unión Interparlamentaria (UIP) en la Cumbre Mundial sobre la Sociedad de la Información celebrada en 2005.

El Cuarto Foro Parlamentario se centrará en las responsabilidades en materia de representación, elaboración de leyes y control que incumben a los miembros de los parlamentos en la esfera de la ciberseguridad. Abordará los especiales retos que plantean el uso ilícito de la información y las tecnologías de la comunicación, como la salvaguardia de los ciudadanos en el entorno conectado, la protección de información, datos e infraestructuras estatales, y la respuesta transnacional a la ciberdelincuencia.

El objetivo del Foro es profundizar el diálogo entre los legisladores sobre las diferentes prioridades estratégicas y políticas aplicadas a nivel nacional, bosquejar una amplia perspectiva de los diferentes compromisos nacionales encaminados a responder a los retos mencionados, delinear la función y responsabilidades de los parlamentos en sus funciones legislativas y de control en relación con el tema de la ciberseguridad, identificar buenas prácticas parlamentarias y formular recomendaciones para que las legislaturas adopten las medidas pertinentes.

6 Estudio: *Information and Communication Technologies and Human Rights*, Parlamento Europeo, junio de 2010, EXPO/B/DROI/2009/24, www.europarl.europa.eu/activities/committees/studies.do?language=EN

Lugar y estructura de la reunión

El Foro Parlamentario se celebrará los días 18,19 y 20 de mayo de 2011 en la sede de la Organización Internacional del Trabajo en Ginebra (Suiza). Comenzará a las 15.00 horas del viernes 18 mayo, con la ceremonia inaugural, y se clausurará a las 13.00 horas del viernes 20 de mayo de 2011.

El Foro se estructurará en torno a una serie de sesiones plenarias en las que habrá presentaciones de expertos y legisladores de diferentes países. En cada sesión se reservará tiempo suficiente para intervenciones del público, diálogos interactivos y debates abiertos entre los miembros de los parlamentos.

Participación

Está previsto que asistan al Foro Parlamentario unos 150 parlamentarios de todo el mundo encargados de temas relacionados con la sociedad de la información. Se prevé que los presidentes de comisiones parlamentarias con competencias en materia de ciencia y tecnología y/o cuestiones de seguridad encabecen las delegaciones y participen activamente en los debates con sus homólogos de otros países y regiones.

Se contará también con la presencia de representantes y directivos de organizaciones internacionales, así como de expertos de organismos internacionales, gobiernos, empresas de TIC y el mundo académico.

Contribuciones de los parlamentarios

Con objeto de que el Foro se vea enriquecido con información sobre las experiencias de los países, se insta encarecidamente a las delegaciones a que presenten un breve informe con antelación, explicando las medidas adoptadas a nivel nacional para abordar cuestiones mundiales de ciberseguridad. Las contribuciones deben centrarse en la función que desempeñan los parlamentos, las comisiones parlamentarias y los legisladores al representar las opiniones de los votantes, propiciar los procesos de elaboración de leyes y políticas y garantizar el control de las actividades dirigidas por el gobierno.

Las contribuciones deben presentarse en español, francés o inglés, y ceñirse al modelo de la planilla que se adjunta, que también está disponible en la página web del Foro.

Idiomas

Los idiomas de trabajo de la reunión serán el español, el francés y el inglés. Se dispondrá de interpretación simultánea en los tres idiomas.

Organizadores

El Cuarto Foro Parlamentario será organizado conjuntamente por el Departamento de Asuntos Económicos y Sociales (DAES) de las Naciones Unidas, la Unión Internacional de Telecomunicaciones (UIT) y la Unión Interparlamentaria (UIP), a través del Centro Mundial para las TIC en el Parlamento.

Naciones Unidas: Departamento de Asuntos Económicos y Sociales (DAES/UN)

El Departamento de Asuntos Económicos y Sociales (DAES) de las Naciones Unidas promueve y apoya la cooperación internacional con miras al logro del desarrollo para todos, y presta asistencia a los gobiernos en la elaboración de programas y la adopción de decisiones en materia de desarrollo a escala internacional. El DAES proporciona una amplia gama de material para el análisis y presta asesoramiento político, elementos que sirven a los países desarrollados y en desarrollo como valiosa fuente de referencia y herramienta para la toma de decisiones, en particular, para plasmar los compromisos internacionales en políticas y medidas nacionales y supervisar los avances hacia la consecución de los objetivos de desarrollo internacionalmente convenidos, entre otros, los Objetivos de Desarrollo del Milenio.

Unión Internacional de Telecomunicaciones (UIT)

La UIT es el organismo principal de las Naciones Unidas encargado de cuestiones relativas a las tecnologías de la información y la comunicación (TIC), y el centro de enlace mundial de los gobiernos y el sector privado para la creación de redes y servicios. Desde hace casi 145 años, la UIT coordina el uso mundial compartido del espectro radioeléctrico, promueve la cooperación internacional en la asignación de órbitas satelitales, procura mejorar la infraestructura de las telecomunicaciones en el mundo en desarrollo, elabora normas mundiales que garantizan la interconexión continua de una amplia gama de sistemas de comunicación, y colabora en la resolución de retos mundiales, tales como la mitigación del cambio climático y el reforzamiento de la ciberseguridad. La UIT, con sede en Ginebra (Suiza), cuenta con 191 Estados Miembros.

Unión Interparlamentaria (UIP)

La Unión Interparlamentaria es la organización internacional de los parlamentos. Creada en 1889, la UIP es el centro de coordinación del diálogo parlamentario del mundo entero y trabaja por la paz y la cooperación entre los pueblos y por el firme establecimiento de una democracia representativa. Actualmente, cuenta con 151 parlamentos y 8 asociaciones miembros. La sede de la UIP está ubicada en Ginebra (Suiza).

Centro Mundial para las TIC en el Parlamento

El Centro Mundial para las TIC en el Parlamento es una iniciativa conjunta del Departamento de Asuntos Económicos y Sociales (DAES) de las Naciones Unidas, la Unión Interparlamentaria y un grupo de parlamentos nacionales y regionales, emprendida en el marco del proceso de la Cumbre Mundial sobre la Sociedad de la Información celebrada en noviembre de 2005. Sus objetivos son: a) impulsar el papel de los parlamentos y los legisladores en la promoción de la sociedad de la información, y b) fortalecer la capacidad de los parlamentos para aprovechar las herramientas de las TIC y desempeñar mejor sus funciones democráticas, poniéndolas al servicio del proceso institucional y la cooperación interparlamentaria.