Naciones Unidas A/59/116

Asamblea General

Distr. general
23 de junio de 2004
Español
Original: árabe/chino/español/
inglés

Quincuagésimo noveno período de sesiones
Tema 62 de la lista preliminar*
Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional

Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional

Informe del Secretario General

Índice

* A/59/50 y Corr.1.

04-40707 (S) 230704 260704
0440707

I. Introducción

1. En el párrafo 3 de su resolución 58/32, de 8 de diciembre de 2003, relativa a los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, la Asamblea General invitó a todos los Estados Miembros a que siguieran haciendo llegar al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes: a) la evaluación general de los problemas de la seguridad de la información; b) la determinación de criterios básicos relativos a la seguridad de la información, en particular la injerencia no autorizada en los sistemas de información y de telecomunicaciones y los recursos de la información o la utilización ilícita de esos sistemas, y c) el contenido de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones. En el párrafo 4 de la resolución, la Asamblea General pidió al Secretario General que examinara las amenazas reales y potenciales en el ámbito de la seguridad de la información, y las posibles medidas de cooperación para conjurarlas, y que preparara un estudio, con la asistencia de un grupo de expertos gubernamentales, que se establecería en 2004, y cuyos miembros serían nombrados por él sobre la base de una distribución geográfica equitativa, al igual que con la ayuda de los Estados Miembros que pudieran prestar esa ayuda, y que presentara un informe sobre los resultados del estudio a la Asamblea General en su sexagésimo período de sesiones. El Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional iniciará su trabajo en julio de 2004.

2. En una nota verbal de fecha 18 de febrero de 2004, se invitó a todos los Estados Miembros a que hicieran llegar al Secretario General sus opiniones y evaluaciones sobre el tema. Hasta la fecha se han recibido siete respuestas, cuyos textos se reproducen en la sección II *infra*. Las respuestas adicionales que se reciban se publicarán como adiciones al presente informe.

II. Respuestas recibidas de Estados Miembros

Argentina

[Original: español]
[14 de mayo de 2004]

Situación Actual

1. La República Argentina ha realizado importantes avances en materia de seguridad y privacidad de los datos. En el plano normativo, la Ley No. 25326 de protección de los datos personales es una de las más modernas de su tipo en el mundo y su contralor se encuentra a cargo de una dirección creada específicamente a dichos fines en el ámbito de Ministerio de Justicia. Por otro lado, se encuentran en estado avanzado varios proyectos de ley de delitos informáticos en tratamiento en el Congreso de la Nación.

2. También se ha avanzado en la legislación relativa a la firma digital, buscando dotar de validez legal y seguridades técnicas a la documentación electrónica, a fin de garantizar su autoría e integridad. La Argentina ha sido pionera en la materia y a

la fecha se están dando los últimos pasos para la implementación de la infraestructura nacional de claves públicas.

3. En particular, el Estado argentino ha realizado importantes avances en materia de seguridad informática. En esta línea, la Oficina Nacional de Tecnologías Informáticas tiene asignada la responsabilidad primaria de entender, asistir y supervisar en los aspectos relativos a la seguridad y privacidad de la información digitalizada y electrónica del sector público nacional.

4. En el ámbito de esa Oficina funciona el ArCERT (Coordinación de Emergencias en Redes Teleinformáticas de la Administración Pública Nacional), equipo de respuestas ante incidentes en redes de organismos públicos, cuyo objetivo principal es elevar los umbrales de seguridad en el sector público. En esta línea se efectúa el tratamiento de los incidentes de seguridad reportados, se emiten alertas en forma preventiva y correctiva, se han desarrollado herramientas específicas de seguridad, se están dictando cursos en la materia destinados a agentes y funcionarios del sector público y se está avanzando en el desarrollo de políticas de seguridad modelo para el Estado.

Evaluación general de los problemas

5. La seguridad informática presenta varios aspectos cuya solución representa un verdadero desafío, atento a la complejidad creciente de los problemas a resolver como resultado del avance tecnológico.

6. Los principales problemas pueden dividirse en tres clases:

Ataques contra la información en sí misma;

Uso indebido de recursos informáticos;

Delitos cibernéticos.

7. En lo referente a la información, las nuevas tecnologías hacen cada vez más difícil mantener las tres principales propiedades de la información: confidencialidad, integridad y disponibilidad. A su vez dentro de los problemas de la información en sí, hay dos principales clases que requieren especial tratamiento: la información personal, que debe administrarse con la mayor reserva para preservar la privacidad de las personas, y la información relativa a las organizaciones, tanto se trate de información comercial, industrial o de organismos o agencias públicos, cuya difusión, modificación o pérdida podría perjudicar objetivos económicos, sociales, políticos, etc.

8. Otro problema normalmente subestimado es el uso indebido de recursos informáticos. Por uso indebido debe entenderse la utilización de los recursos asignados para fines distintos a los autorizados o de manera irracional que implique su abuso, derroche o desaprovechamiento. Por ejemplo, la actual propagación masiva de virus y de otro tipo de intrusiones por Internet, y las contramedidas necesarias, originan costos adicionales muy superiores a los necesarios para el objetivo original de los mismos. Un enfoque preventivo en la materia ahorrará importantes recursos y esfuerzos.

9. Por último, las nuevas tecnologías generan nuevos medios de acceso para la comisión de delitos, tanto para aquellos considerados clásicos, ahora apoyados en nuevas tecnologías, como nuevas variantes inspiradas en los avances tecnológicos.

China

[Original: chino]
[24 de mayo de 2004]

Opiniones de China sobre las cuestiones relativas a la seguridad de la información

1. Los rápidos avances en la información y las telecomunicaciones son un rasgo importante del progreso científico y tecnológico. En la actual situación, caracterizada por la multiplicación de las amenazas para la seguridad, el aumento de los factores de seguridad no tradicionales y la intensificación de las actividades terroristas internacionales, la seguridad de la información se ha convertido en un reto importante relacionado con la seguridad internacional. China apoya los esfuerzos internacionales encaminados a mantener y promover la seguridad de la información en todos los países y el establecimiento de un Grupo de Expertos Gubernamentales de las Naciones Unidas que se encargue de examinar la cuestión de la seguridad de la información y de proponer medidas al respecto.

2. China sostiene que la tecnología de la información debería utilizarse conforme a la Carta de las Naciones Unidas y a otros principios aceptados internacionalmente, así como servir para mantener y promover la paz, la estabilidad y el desarrollo en los planos regional e internacional. Teniendo en cuenta la preponderancia cada vez mayor de las amenazas no tradicionales para la seguridad, los Estados deberían otorgar una gran importancia a los delitos relacionados con la información y el terrorismo. Dado el desigual desarrollo de las telecomunicaciones en los distintos países, la sociedad internacional también debería fortalecer la cooperación en el ámbito de la investigación y la aplicación de la tecnología de la información.

3. China opina que en el marco del Grupo de Expertos Gubernamentales de las Naciones Unidas sobre seguridad de la información todas las partes deberían examinar las amenazas actuales y potenciales en el ámbito de la seguridad de la información y estudiar medios específicos de afrontar esas amenazas. China participará de forma positiva y constructiva en la labor del Grupo de Expertos Gubernamentales de las Naciones Unidas y espera que su trabajo conduzca a unos resultados positivos.

Costa Rica

[Original: español]
[15 de marzo de 2004]

1. El Gobierno de Costa Rica ha de indicarle que el 24 de octubre de 2001 la Asamblea Legislativa de Costa Rica aprobó una reforma al Código Penal titulada “Adición de los artículos 196 bis, 217 bis y 229 bis al Código Penal, Ley No. 4573 para reprimir y sancionar los delitos informáticos”. Dicha reforma ha sido el avance más significativo en los últimos años en lo referente a seguridad informática en Costa Rica.

2. Dicha reforma ha llegado a tipificar tres tipos de delitos informáticos (violación de comunicaciones electrónicas, fraude informático y alteración de datos y sabotaje informático), siendo un avance importante para Costa Rica, en dicha materia, y adaptándose a las necesidades actuales para garantizar la seguridad informática.

3. Adjunto la reforma íntegra para su consideración (véase el apéndice).

Apéndice

Adición de los artículos 196 bis, 217 bis y 229 bis al Código Penal, Ley No. 4573 para reprimir y sancionar los delitos informáticos

8148

La Asamblea Legislativa de la República de Costa Rica

Decreta

Adición de los artículos 196 bis, 217 bis y 229 bis al Código Penal, Ley 4573, para reprimir y sancionar los delitos informáticos

Artículo único. Adiciónense al Código Penal, Ley No. 4573, de 4 de mayo de 1970, los artículos 196 bis, 217 bis y 229 bis, cuyos textos dirán:

Artículo 196 bis. Violación de comunicaciones electrónicas

Será reprimida con pena de prisión de seis meses a dos años, la persona que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere, accese, modifique, altere, suprima, intercepte, interfiera, utilice, difunda o desvíe de su destino, mensajes, datos e imágenes contenidas en soportes: electrónicos, informáticos, magnéticos y telemáticos. La pena será de uno a tres años de prisión, si las acciones descritas en el párrafo anterior, son realizadas por personas encargadas de los soportes: electrónicos, informáticos, magnéticos y telemáticos.

Artículo 217 bis. Fraude informático

Se impondrá pena de prisión de uno a 10 años a la persona que, con la intención de procurar y obtener un beneficio patrimonial para sí o para un tercero, influya en el procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.

Artículo 229 bis. Alteración de datos y sabotaje informático

Se impondrá pena de prisión de uno a cuatro años a la persona que por cualquier medio accese, borre, suprima, modifique o inutilice sin autorización los datos registrados en una computadora.

Si como resultado de las conductas indicadas se entorpece o inutiliza el funcionamiento de un programa de cómputo, una base de datos o un sistema informático, la pena será de tres a seis años de prisión. Si el programa de cómputo, la base de datos o el sistema informático contienen datos de carácter público, se impondrá pena de prisión hasta de ocho años.

Cuba

[Original: español]
[1° de junio de 2004]

Opiniones de la República de Cuba en virtud de lo solicitado en el párrafo 3 de la resolución 58/32 titulada "Los avances de la información y las telecomunicaciones en el contexto de la seguridad internacional"

1. En los apartados a) y b) del párrafo 3 de la resolución 58/32, de fecha 8 de diciembre de 2003, relativa a los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, la Asamblea General invitó a todos los Estados Miembros a que siguieran haciendo llegar al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes: a) la evaluación general de los problemas de la seguridad de la información; b) la determinación de criterios básicos relativos a la seguridad de la información, en particular la injerencia no autorizada en los sistemas de información y de telecomunicaciones y los recursos de la información o la utilización ilícita de esos sistemas, y c) el contenido de los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones.

2. Cuba considera que el uso hostil de las telecomunicaciones, con el propósito declarado o encubierto de subvertir el ordenamiento jurídico y político de los Estados, es una violación de las normas internacionalmente reconocidas en esta materia y una manifestación negativa, irresponsable del empleo de esos medios, cuyos efectos pueden generar tensiones y situaciones desfavorables para la paz y la seguridad internacionales, en directa contravención con los principios y propósitos consagrados en la Carta de las Naciones Unidas.

3. En su párrafo preambular 8, la resolución 58/32 reitera una vez más la preocupación de la Asamblea General ante "la posibilidad de que estos medios y tecnologías se utilicen con fines incompatibles con el objetivo de garantizar la estabilidad y la seguridad internacionales y afecten negativamente a la integridad de la infraestructura de los Estados, en detrimento de su seguridad en las esferas civil y militar". Cuba comparte plenamente dicha preocupación.

4. Los sistemas de información y telecomunicaciones pueden convertirse en armas cuando se diseñan y/o emplean para causar daños a la infraestructura de un Estado.

5. Cuba reitera que todos los Estados deben respetar las normas internacionales y existentes en esta esfera. Los accesos a los sistemas de información o de telecomunicaciones de otro Estado deben corresponderse con los acuerdos de cooperación internacional alcanzados, sobre la base del principio del consentimiento del Estado concernido. Las formas y el alcance de los intercambios deben respetar la legislación del Estado a cuyo sistema se accederá.

6. La seguridad y la paz internacionales pueden ser afectadas por la agresión de un Estado a los sistemas de información o de telecomunicaciones de otros Estados. Lamentablemente, estos procedimientos ya son utilizados como herramientas para la aplicación de políticas hostiles.

7. Cuba sufre ese tipo de agresiones promovidas, consentidas y ejecutadas por el Gobierno de los Estados Unidos desde hace casi 20 años. Desde 1985 y 1990, fechas en que el Gobierno norteamericano estableció ilegalmente una emisora radial y una televisiva, respectivamente, se vienen produciendo afectaciones e interferencias a las transmisiones de radio y televisión cubana.

8. Cada semana, procedente de Estados Unidos se dirigen hacia Cuba 2.227 horas y media de transmisiones de radio y televisión con programación subversiva contra el orden constitucional. Son 29 las frecuencias diferentes que se destinan a programaciones exclusivamente con esos fines, a partir de 18 emisoras de onda media, corta, FM y televisión.

9. En conjunto, se generan desde el número de frecuencias indicadas entre 312 y 315 horas diarias de una programación manipulada políticamente, que nada tiene que ver con la promoción de un libre flujo de la información y las ideas, en tanto se transmiten falsas alegaciones —fabricadas mediante el fraude, la mentira y la tergiversación— y se difunden mensajes dirigidos a promover la ruptura del orden constitucional del país.

10. De las 18 emisoras que participan en la agresión radioelectrónica y televisiva contra Cuba, 15 pertenecen a organizaciones vinculadas o pertenecientes a conocidos elementos terroristas que residen, operan y actúan en territorio norteamericano, con pleno conocimiento y consentimiento de las autoridades de la Administración Federal de los Estados Unidos.

11. De estas emisoras, 12 existen específicamente contra Cuba. Entre ellas, se encuentran las mal llamadas televisión y radio Martí. Ellas son propiedad del Gobierno de los Estados Unidos, que destina 35 millones de dólares anuales a esta guerra radioelectrónica contra Cuba.

12. Como una nueva y peligrosa provocación, el Gobierno de los Estados Unidos anunció en mayo de 2004 que procedería a desplegar la plataforma aérea “EC-130 Comando Solo” y a asignar fondos adicionales para comprar y reacondicionar una plataforma aérea dedicada a la transmisión hacia Cuba de las llamadas Radio y TV Martí.

13. En las transmisiones ilegales contra Cuba se tergiversa la realidad de nuestro país, se alienta la emigración ilegal y en condiciones peligrosas, se incita al desacato y la desobediencia civil, se incita a la violencia, a la realización de acciones terroristas y a la destrucción del orden institucional y legal establecidos por la Constitución de la República de Cuba, refrendada por el voto positivo de más del 96% de los cubanos.

14. El empleo de información con un marcado interés de subvertir el orden interno de los Estados, violar su soberanía y realizar actos de intromisión e interferencia en sus asuntos internos, constituye una acción ilegal en virtud del derecho internacional y atenta contra el disfrute del derecho a la libre determinación de los pueblos.

15. Estas transmisiones no solamente violan la soberanía de Cuba, sino que constituyen flagrantes transgresiones a las regulaciones establecidas por la Junta Internacional de Registros de Frecuencias de la Unión Internacional de Telecomunicaciones, en especial del numeral 23.3 de su Reglamento de Telecomunicaciones, que prohíbe las transmisiones televisivas más allá de los límites nacionales, por lo cual constituyen acciones violatorias del derecho internacional.

16. Con tales transmisiones de televisión también se viola el preámbulo de la Constitución de la Unión Internacional de Telecomunicaciones, al realizar actividades que no facilitan las relaciones pacíficas, la cooperación internacional entre los pueblos y el desarrollo económico y social por medio del buen funcionamiento de las telecomunicaciones.

17. Cuba considera necesario llamar la atención una vez más sobre los siguientes aspectos, estrechamente asociados a una plena potenciación de las telecomunicaciones como instrumento de fortalecimiento de la paz y la seguridad internacionales:

a) Todos los Estados deben abstenerse de la aplicación de medidas coercitivas unilaterales, contrarias al derecho internacional, que impongan restricciones al Estado afectado en cuanto al acceso a las tecnologías y a las redes internacionales de intercambio de información y comunicaciones;

b) Los sistemas de certificación y eventuales sanciones a cualquier Estado en cuanto al acceso a las tecnologías de telecomunicaciones u otras estrechamente vinculadas por razones de amenaza a la paz y a la seguridad internacionales, deben tener una naturaleza multilateral y estar planteados sobre patrones acordados por la comunidad internacional;

c) La cooperación internacional en la materia debe ser fortalecida, movilizando los recursos necesarios para asistir a los países en desarrollo en el fortalecimiento y expansión de sus sistemas de telecomunicaciones;

d) Las medidas legislativas y de otra índole, tanto a nivel nacional como internacional, deberán adoptarse urgentemente con el objetivo de prohibir la indebida concentración en manos de personas naturales de la propiedad y el control de los medios de telecomunicaciones —así como de otros medios de información y comunicaciones— a partir de su negativo impacto en la necesaria diversidad de las fuentes de información y su potencialidad como herramienta de propaganda contra la paz y de incitación a la guerra;

e) Un sistema multilateral, intergubernamental, democrático y transparente en la administración y control de Internet y otras redes internacionales de información y comunicaciones deberá establecerse. El carácter intergubernamental del sistema de escrutinio es un requisito vital;

f) Los sistemas de control y monitoreo de las telecomunicaciones y otras formas de comunicaciones internacionales, deben tener un carácter multilateral, transparente, con claras responsabilidades y procedimientos de escrutinio público, con el objetivo de ponerle fin a las violaciones a la soberanía, a la seguridad de muchos Estados, e inclusive a la privacidad del individuo, cometidas por los sistemas globales de espionaje operados por países industrializados y, en particular, por los Estados Unidos;

g) Debe promoverse el desarrollo de garantías efectivas a favor de la diversidad cultural y de la eliminación de toda forma de discriminación o incitación al odio en el contenido de la información difundida en los sistemas de telecomunicaciones a nivel internacional.

Georgia

[Original: inglés]
[18 de mayo de 2004]

Los avances en la información y las comunicaciones en Georgia en el contexto de la seguridad internacional

1. El estado actual de la seguridad de la información y las telecomunicaciones en Georgia

1.1 El sistema de seguridad de la información de Georgia está en fase de preparación.

1.2 El sistema nacional de seguridad de la información ha sido elaborado por el Ministerio de Infraestructuras y Desarrollo y la Comisión Nacional de Comunicaciones.

1.3 La iniciativa se está llevando a cabo sin que se le hayan destinado fondos específicos.

2. Estado de los trabajos

El grupo de trabajo encargado de esta iniciativa está integrado por los siguientes miembros:

- Ministerio de Infraestructuras y Desarrollo de Georgia: Departamento de Telecomunicaciones y de Tecnologías de la Información;
- Comisión Nacional de Comunicaciones de Georgia: Departamento Técnico.

3. Los principios básicos de la política de Georgia relativa al sistema de seguridad de la información son los siguientes:

3.1 Las directrices generales en materia de seguridad de la información se definen en el Programa de Informatización de Georgia, que se encuentra en fase de elaboración.

3.2 La estrategia de seguridad para los sistemas de información públicos, gubernamentales y empresariales, así como la infraestructura de las telecomunicaciones, deberían basarse en el sistema nacional de normas de seguridad de la información.

3.3 El sistema de normas de seguridad de la información de Georgia se basa en la armonización de normas internacionales de la Organización Internacional de Normalización, la Unión Internacional de Telecomunicaciones y el Instituto Europeo de Normas de Telecomunicaciones.

3.4 A nivel empresarial, la política de seguridad de la información se basa en una serie de normas y recomendaciones metódicas con certificación voluntaria conforme a la norma ISO 17799.

4. La participación de Georgia en la sociedad global de la información debería ofrecer las siguientes oportunidades:

4.1 Establecimiento de una infraestructura y un espacio de información conjuntos y participación de Georgia en los procesos internacionales, incluso en el desarrollo de un sistema internacional de seguridad de la información.

4.2 Globalización integrada, basada en las normas internacionales sobre información y compatible con la participación de Georgia en la Organización Mundial del Comercio, las Naciones Unidas y otras organizaciones internacionales.

4.3 Participación en la economía postindustrial mundial sobre la base de los principios de la cooperación y el acceso a la información, y superación de la brecha en materia de información entre Georgia y la comunidad internacional de la información.

4.4 Aumento de la seguridad de la información en Georgia.

5. Funciones principales del Ministerio de Infraestructuras y Desarrollo de Georgia en la esfera de la seguridad de la información

5.1 Detección de las deficiencias en las normas sobre telecomunicaciones, supervisión y examen de los resultados de los trabajos de las organizaciones internacionales de normalización, sistemas de certificación de la calidad, y seguridad del medio ambiente y de la información.

5.2 Adaptación de los programas locales e internacionales y la estrategia de desarrollo de las comunicaciones a los requisitos de las organizaciones internacionales; cooperación con las iniciativas internacionales y los proyectos regionales de seguridad.

6. Mejora de la seguridad de la información nacional en Georgia

6.1 Para la eficaz ejecución del programa de información y del sistema de seguridad de la información es preciso destinar fondos específicamente a estas actividades y disponer de un apoyo internacional.

6.2 La ayuda de las organizaciones internacionales es importante en ámbitos como:

- La investigación relativa a la infraestructura de las telecomunicaciones y la migración a redes de nueva generación;
- El análisis de las condiciones y la comparabilidad de los sistemas nacionales de normas sobre seguridad de la información;
- La elaboración de programas y técnicas de seguridad de la información en varias esferas de actividad económica y social.

7. Cooperación con las organizaciones internacionales

- La Unión Internacional de Telecomunicaciones y la Comunidad Regional para las Comunicaciones;
- Las Naciones Unidas;
- La Comisión Económica y Social para Asia y el Pacífico, la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo y la Organización Mundial del Comercio.

8. Proyectos, seminarios y otras actividades

8.1 Unión Internacional de Telecomunicaciones: proyecto de un sistema de protección del Ministerio de Infraestructuras y Desarrollo de Georgia contra el acceso no autorizado.

Organizadores: Oficina de Desarrollo de las Telecomunicaciones, Unión Internacional de Telecomunicaciones, “Utimaco”, Gobierno de Bulgaria, Departamento de Telecomunicaciones y Tecnologías de la Información.

8.2 Seminarios de capacitación sobre el desarrollo de la infraestructura para los sectores comercial y financiero de Georgia.

- Creación de un sistema empresarial con el apoyo de las nuevas tecnologías de la información y las comunicaciones;
- Comercio electrónico; desarrollo de la tecnología de la información y las comunicaciones para los sectores comercial y financiero, desarrollo de un sistema financiero y comercial electrónico, un sistema de banca electrónica y un sistema de pagos electrónicos;
- Examen de los problemas, incluso desarrollo de una infraestructura nacional para los sectores comercial y financiero.

El Líbano

[Original: árabe]
[27 de mayo de 2004]

El Estado libanés, habida cuenta del desarrollo y la aplicación de las tecnologías de la información y de las comunicaciones por cable e inalámbricas, vela por que esas tecnologías no se utilicen para fines contrarios a la estabilidad y seguridad internacionales. Considera indispensable prohibir el uso de recursos o tecnologías de la información con fines delictivos o terroristas y coopera con las Naciones Unidas en la aplicación de sus resoluciones para proteger la seguridad y confidencialidad de la información y prevenir por todos los medios su mala utilización.

Reino Unido de Gran Bretaña e Irlanda del Norte

[Original: inglés]
[14 de mayo de 2004]

1. El Reino Unido de Gran Bretaña e Irlanda del Norte acoge con beneplácito el compromiso de la comunidad de las Naciones Unidas de afrontar las consecuencias de nuestra creciente dependencia de las redes de comunicación y los sistemas de información, que nos hacen vulnerables a las amenazas. La seguridad de la información es crucial para el crecimiento de la economía mundial y su importancia se reflejó en los principios y el plan de acción que aprobó la Cumbre Mundial sobre la Sociedad de la Información al concluir su primera fase.

2. Los principios aprobados comprenden la promoción, elaboración e instauración de una cultura mundial de seguridad cibernética en cooperación con todos los interesados y los órganos internacionales de expertos, así como el apoyo a esos esfuerzos mediante el aumento de la cooperación internacional. El Reino Unido está convencido de que la mejor manera de cumplir los objetivos de seguridad de los países consiste en promover una cultura mundial de seguridad cibernética, como se describe en los Principios de la Cumbre Mundial sobre la Sociedad de la Información, los Principios del Grupo de los Ocho para proteger las infraestructuras de

información esenciales, y la resolución 58/199 de la Asamblea General de las Naciones Unidas.

3. No obstante, el Reino Unido considera que no se necesita un instrumento multilateral que restrinja la elaboración o utilización de determinadas tecnologías civiles o militares. Con respecto a las aplicaciones militares de las tecnologías de la información ese tipo de instrumento es innecesario. La Ley de conflictos armados, en particular los principios de necesidad y proporcionalidad consagrados en ella, ya regula el uso de esas tecnologías. Además, un instrumento de ese tipo podría interferir con la libre circulación de la información, que la Cumbre Mundial sobre la Sociedad de la Información reconoció como principio fundamental de la sociedad de la información.

Nociones básicas y conceptos pertinentes

4. Debemos considerar los riesgos que afectan a las redes y los sistemas de información en función de la amenaza y la vulnerabilidad. La amenaza es algo que cambia constantemente, pero está claro que se ha vuelto un fenómeno más complejo en los últimos años. Los agentes estatales representan sólo una pequeña parte de la amenaza para los sistemas de información. En años recientes han causado mayor preocupación las actividades de terroristas, delincuentes organizados y piratas informáticos que han intentado acceder a distintos sistemas de forma inapropiada o perturbar el funcionamiento de las redes. Para reforzar la seguridad cibernética en todo el mundo es necesario asegurar que los ataques contra los sistemas y las redes de información estén tipificados como delitos por las leyes penales. El Convenio del Consejo de Europa sobre el Delito Cibernético es el mejor modelo sobre el que basar el proceso de tipificación del delito cibernético.

5. Ahora bien, el análisis de las amenazas es sólo un aspecto de la seguridad cibernética. El Reino Unido opina que la defensa de las redes y los sistemas de información es en gran medida independiente de la fuente de la amenaza y que, por lo tanto, la cooperación internacional debe estar encaminada, a corregir las vulnerabilidades, que pueden ser tecnológicas, relacionadas con los programas o los protocolos, pero también pueden surgir de errores de los usuarios cuando mediante técnicas de “ingeniería social” o “phishing” (uso de páginas web falsas) se les engaña para que proporcionen información de seguridad. Nuestro reto principal consiste en cambiar la cultura cibernética, es decir, la forma en que se elaboran, despliegan y utilizan las redes y los sistemas de información. Las “Directrices para la seguridad de los sistemas y redes de información: hacia una cultura de la seguridad”, de la Organización de Cooperación y Desarrollo Económicos (OCDE), proporcionan una sólida base para iniciar este cambio cultural.

Aplicación de los conceptos pertinentes: enfoque del Reino Unido

6. En 2003, el Reino Unido adoptó una estrategia nacional para la seguridad de la información, que abarca la protección de los sistemas fundamentales de información y el refuerzo de las redes. La estrategia se centra en la protección de los sistemas y los recursos informáticos gubernamentales pero reconoce la importancia de colaborar con el sector privado e incluye un claro elemento de difusión a las empresas y a los ciudadanos. También reconoce la importancia de colaborar con otros países para lograr un espacio cibernético más seguro.

7. El Gobierno se ha dotado de nuevas estructuras para aplicar la estrategia, con la participación de los Ministerios de Interior, Industria y Defensa y el nombramiento en cada departamento estatal de un encargado de riesgos. Para apoyar la estrategia, también se está desarrollando la capacidad técnica de los expertos gubernamentales a fin de prever y responder a los problemas de seguridad de la información. La estrategia también reconoce la importancia de la investigación y la innovación, y sus encargados deberán publicar en junio de 2004 un gran estudio sobre enfoques a la seguridad cibernética a largo plazo.

8. La estrategia del Reino Unido comprende tres iniciativas fundamentales. En 1999, el Reino Unido estableció un Centro Nacional de Coordinación de la Seguridad de las Infraestructuras, iniciativa de la que se encargan múltiples organismos y que actualmente goza de muy buena reputación internacional por su eficaz labor de protección de las infraestructuras básicas. El Centro fomenta el intercambio de información entre comunidades de intereses, coordina la difusión de alertas en tiempo real sobre la base de contactos internacionales y desempeña una función primordial en la detección y corrección de vulnerabilidades en los protocolos.

9. El Reino Unido ha ejercido un papel crucial en la elaboración de normas de gestión de la seguridad de la información, incluidas las directrices sobre la gestión de la seguridad de la información (ISO/CEI/17799), que originalmente era una norma británica y que se está aceptando rápidamente como la norma principal en este ámbito. Estas normas adoptan un enfoque de la seguridad de la información basado en la vulnerabilidad o el riesgo, lo que permite a las organizaciones integrar plenamente la gestión de la seguridad de la información.

10. Con el fin de luchar contra los delitos cibernéticos, el Reino Unido está elaborando una estrategia contra el delito electrónico que se basa en el Convenio del Consejo de Europa y en la legislación de la Unión Europea. Además, el conjunto de las instituciones encargadas de hacer cumplir la ley en el Reino Unido ha comenzado a reflejar la nueva naturaleza del delito cibernético con la creación de una entidad nacional, la Dependencia Nacional de Lucha contra el Delito de Alta Tecnología, junto con unidades de especialistas en las fuerzas de policía locales.

Aplicación de los conceptos pertinentes: potencial de cooperación internacional

11. La Cumbre Mundial sobre la Sociedad de la Información subraya la importancia de la cooperación internacional con miras a elevar al máximo el potencial de la sociedad de la información. La resolución 58/32 de la Asamblea General de las Naciones Unidas proporciona una oportunidad para crear una cultura de seguridad cibernética que proteja los intereses de los gobiernos, las empresas y los ciudadanos reduciendo al mínimo el riesgo de perturbación de los sistemas y protegiendo la libre circulación de la información. Las directrices de la OCDE constituyen un sólido modelo de principios que podrían contribuir a fomentar ese tipo de cultura y deberían formar la base de nuestro enfoque de la seguridad cibernética.

12. El Reino Unido acoge con beneplácito el compromiso de la comunidad de las Naciones Unidas con la cuestión de la seguridad de la información y opina que la Organización puede contribuir al desarrollo de una cultura de seguridad cibernética centrando la atención en las siguientes cuestiones:

- Elaboración e intercambio de mejores prácticas;
- Establecimiento de un enfoque básico común para la tipificación de los delitos cibernéticos, sobre la base del Convenio del Consejo de Europa;
- Refuerzo de la colaboración en tiempo real entre las autoridades nacionales en lo que respecta a la detección de amenazas y vulnerabilidades, la investigación y el enjuiciamiento de los delincuentes;
- Elaboración de un enfoque más coherente para eliminar las vulnerabilidades de los sistemas de información.