Naciones Unidas A/58/373

Asamblea General

Distr. general
17 de septiembre de 2003
Español
Original: español/francés/inglés/ruso

Quincuagésimo octavo período de sesiones
Tema 69 del programa provisional*
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/58/150.

03-52343 (S) 091003 101003

I. Introducción

1. En el párrafo 3 de su resolución 57/53, 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 los peligros reales y potenciales en la esfera de la seguridad de la información, y las posibles medidas de cooperación para reducirlos, 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.

2. En una nota verbal de fecha 18 de febrero de 2003, 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 los Estados Miembros

Bolivia

[Original: español]
[17 de junio de 2003]

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

1. Bolivia expresa su preocupación que el avance tecnológico sea utilizado con fines incompatibles a la estabilidad y seguridad internacional, afectando negativamente a la integridad de los Estados en detrimento de su propia seguridad en las esferas militares y civiles.

2. Bolivia destaca la necesidad de impedir la utilización de los recursos que ofrece la tecnología de la información para fines delictivos o terroristas.

3. En este sentido, expresa la consideración de criterios básicos relativos a la seguridad de la información y la injerencia no autorizada en los sistemas conexos.

Importancia de la información

4. Cuando se habla de información directa e indirectamente nos referimos a los sistemas informáticos y las telecomunicaciones (nuevas tecnologías, nuevas aplicaciones-software, nuevos dispositivos-hardware, nuevas formas de elaborar la información cada vez más consistente, confiable y veloz), con la consideración primaria del riesgo y la seguridad de las mismas.

5. Es necesario tener presente que el lugar donde se centraliza la información con frecuencia pude ser el más valioso y al mismo tiempo el más vulnerable.

6. Las telecomunicaciones por su vulnerabilidad, enfoca la INTERNET y la telefonía. La INTERNET está directamente relacionada a los sistemas informáticos. La telefonía se divide en celular y de hilos. La celular convive inmediatamente con un espacio de propagación común (por donde las ondas de radio transitan), donde los usuarios están inmersos al tráfico e interceptación telefónica.

Crónica del crimen o delitos en los sistemas de información

7. Los delitos incidentales y accidentales cometidos utilizando las computadoras y los receptores han crecido en tamaño, forma y variedad. En la actualidad los delitos cometidos son descubiertos en un alto porcentaje de forma casual (fraudes, falsificación y venta de información).

8. En el manejo de los sistemas informáticos mencionamos al virus informático como un programa elaborado accidental o intencionalmente, que requiere de especial atención y que debe ser contrarrestado con estrictos procedimientos de operación.

9. Es importante destacar en la comisión de los delitos, al encontrar los problemas se debe atacar la causa e inmediatamente plantear soluciones, entras las causas de mayor riesgo podemos citar: el beneficio personal, el síndrome de Robin Hood, odio a la organización, trastornos mentales y la deshonestidad, entre las causas de menor riesgo está el beneficio de la organización y los juegos.

Paradigmas organizacionales en cuanto a seguridad

10. Los paradigmas desempeñan un papel importante en la actual filosofía de la ciencia, de los mismos se desprenden las reglas que rigen las investigaciones.

11. Entre los principales paradigmas se pueden mencionar los siguientes: la responsabilidad de Auditoría de un sistema es del usuario y del Departamento de Auditoría Interna, los sistemas de seguridad no consideran la posibilidad de fraude interno, los accidentes son poco probables que sucedan a la institución, siempre existen fallas porque ningún sistema es perfecto, además de muchos otros.

Estableciendo el riesgo

12. Es importancia crear una conciencia en los usuarios de la organización sobre el riesgo que corre la información y comprender que la seguridad es parte de su trabajo. Para esto se debe establecer el costo y la calidad del sistema de seguridad, clasificar su instalación en términos de riesgo, identificar las aplicaciones con alto riesgo, cuantificar el impacto de la suspensión del servicio y formular las medidas de seguridad necesarias.

13. Cuando se ha definido el grado de riesgo se debe elaborar una lista con las medidas preventivas que se deben tomar y las medidas correctivas en caso de desastre, señalando la prioridad de cada una de ellas.

14. Se debe considerar y cuantificar el riesgo a nivel institucional, estatal y regional, mencionando los programas de soporte en cuanto a su disponibilidad y recuperación.

Consideraciones de un sistema de seguridad integral

15. Desarrollar un sistema de seguridad significa "planear, organizar, coordinar, dirigir y controlar las actividades relacionadas a mantener y garantizar la integridad de los recursos implicados en la función informática, así como el resguardo de los activos de la institución, del Estado y la Región".

16. Para esta situaciones debemos definir los elementos administrativos, las políticas de seguridad, organizar y distribuir las responsabilidades, establecer los procedimientos de emergencias, definir los objetivos de seguridad, realizar un diagnóstico de la situación de riesgo y seguridad de la información y finalmente elaborar un programa de seguridad.

Cuba

[Original: español]
[28 de mayo de 2003]

1. Cuba siempre ha apoyado las resoluciones sobre "Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional", desde que el tema comenzó a ser objeto de examen en la Primera Comisión de la Asamblea General de las Naciones Unidas en 1998.

2. La inscripción del tema en la agenda de la Asamblea General demuestra que la comunidad internacional ha tomado conciencia de los potenciales peligros para la paz y la seguridad internacionales, cuando las tecnologías de la información no son utilizadas con fines pacíficos.

3. El proceso preparatorio y la celebración misma de la Cumbre Mundial sobre la Sociedad de la Información, en sus dos etapas, Ginebra 2003 y Túnez 2005, ha colocado el tema que atiende la resolución de la referencia y otros que están estrechamente vinculados a la misma, en un lugar prioritario en la atención de la comunidad internacional.

4. El uso hostil de las telecomunicaciones, con el propósito declarado o encubierto de subvertir el ordenamiento jurídico y político de los Estados, es una manifestación negativa del empleo de esos medios cuyos efectos pueden generar tensiones y situaciones desfavorables para la paz y la seguridad internacionales, en franca contradicción con los principios y propósitos consagrados en la Carta de las Naciones Unidas.

5. La resolución 57/53 expresa explícitamente que la difusión y la utilización de las tecnologías y de los medios de información repercuten en los intereses de toda la comunidad internacional y que una amplia cooperación internacional contribuirá a lograr una eficacia óptima.

6. En su párrafo preambular 8, la resolución expresa “preocupación 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 la integridad de la infraestructura de los Estados, en detrimento de su seguridad en las esferas civil y militar”.

7. Por su parte, el párrafo dispositivo 3 b) solicita opiniones y observaciones de los Estados sobre 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 información o la utilización ilícita de esos sistemas”.

8. Cuba entiende por “injerencia no autorizada” el empleo de estos sistemas al margen de los procedimientos y normas acordados internacionalmente, especialmente en el marco de la Unión Internacional de Telecomunicaciones y en contravención de las regulaciones nacionales correspondientes.

9. Los Estados que aún no lo hayan hecho, deben adoptar todas las medidas necesarias para fortalecer dichas regulaciones nacionales.

10. Resulta además indispensable revisar periódicamente las regulaciones internacionales en la materia, habida cuenta de la velocidad con que se desarrollan las tecnologías correspondientes, de modo que su efectividad y eficacia marchen a la par de ese desarrollo.

11. 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. Por ejemplo, la agresión de redes nacionales con software foráneos o desde fuentes internas del propio Estado, pero promovidas o concebidas desde el extranjero; las transmisiones radiales o televisivas dirigidas a promover la ruptura del orden social y la institucionalidad constitucional de otro Estado al que se envían esas señales; las acciones dirigidas a la interferencia, daño o paralización de los servicios de radiodifusión de otros Estados, etc.

12. 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, teniendo en cuenta como piedra angular el principio del consentimiento del Estado concernido. Las formas y alcance de los intercambios, deben respetar la legislación del Estado a cuyo sistema se accederá.

13. La seguridad y la paz internacionales pueden verse dañadas 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.

14. 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. Cada semana, estas emisoras gubernamentales y otras, transmiten hacia nuestro país más de 2.220 horas de programación subversiva contra el orden constitucional. Son 24 las frecuencias que se destinan a programaciones exclusivamente con esos fines.

15. En esa agresión radial y televisiva el Gobierno de los Estados Unidos ha invertido desde 1990 más de 20 millones de dólares al año.

16. Tal y como se dio a conocer en Declaración del Ministerio de Relaciones Exteriores de la República de Cuba de fecha 22 de mayo de 2003, el Gobierno de los Estados Unidos ha iniciado nuevas acciones que constituyen una escalada en la agresión radioelectrónica y televisiva que viene llevando a cabo contra Cuba desde hace décadas.

17. La emisora de radio creada y operada por el Gobierno estadounidense con el objetivo de promover la subversión en Cuba, transmitió el pasado 20 de mayo de 2003 utilizando cuatro nuevas frecuencias, hecho que provocó interferencias y afectaciones a las transmisiones radiales cubanas.

18. Estos actos constituyen una franca y grosera violación del derecho internacional y las normas y regulaciones establecidas por la Unión Internacional de Telecomunicaciones (UIT), organización internacional que fuera constituida con el objetivo de promover el buen funcionamiento de las telecomunicaciones en todo el mundo y, en particular, a su Reglamento de Radiocomunicaciones.

19. En horas de la tarde del mismo día 20 de mayo, la señal televisiva transmitida con iguales propósitos hacia Cuba por los servicios oficiales de propaganda norteamericanos, utilizando un avión EC-130 de las Fuerzas Armadas de los EE.UU., transmitió de seis a diez de la noche, utilizando canales asignados legalmente a estaciones cubanas de televisión e inscritas debidamente en la ya citada organización internacional.

20. Esta acción es también violatoria del derecho internacional y de las normas acordadas por todos los Estados en el marco 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.

21. Estas transmisiones de televisión también violan 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.

22. Cuba rechaza y denuncia por tanto, la tolerancia con que las autoridades norteamericanas han actuado con relación a las actividades del terrorista José Basulto y sus intentos de transmitir señales de televisión hacia territorio cubano. A pesar de que se informó oportunamente por los canales diplomáticos que se había alertado al Sr. Basulto de que cualquier transmisión hacia Cuba sería considerada una violación de la ley norteamericana y en consecuencia se actuaría contra él, este connotado terrorista voló libremente el pasado 20 de mayo y si no transmitió, se debió a problemas con el transmisor que iba a utilizar y no a las acciones de las autoridades estadounidenses, que actuaron en franca complicidad.

23. En virtud del numeral 15.34 del propio Reglamento de Radiocomunicaciones de la UIT, la agresión televisiva de Estados Unidos constituye una interferencia perjudicial, provocada por una estación de televisión operando en el canal 13 de VHF (210 a 216 MHz), que afectó severamente servicios de televisión cubanos debidamente registrados en dicho canal.

24. Las autoridades cubanas en materia de radiocomunicaciones han denunciado el hecho ante la Comisión Federal de Comunicaciones (FCC) del Gobierno de los Estados Unidos, dejando claros todos los parámetros técnicos y legales que han sido groseramente violados.

25. Cuba está procediendo igualmente a denunciar los hechos descritos ante el Secretario General de la Unión Internacional de Telecomunicaciones (UIT) y solicitando la adopción de las medidas correspondientes en estos casos.

26. Cuba considera necesario fortalecer el marco jurídico internacional en materia de información y telecomunicaciones. Igualmente considera imprescindible que se respete el orden internacional ya establecido en la materia, en virtud del respeto irrestricto al derecho internacional y la Carta de las Naciones Unidas que debe primar en las relaciones entre los Estados. En tal sentido, ya existen principios, regulaciones y procedimientos internacionales afines que deben ser respetados.

27. Debe trabajarse por diseñar directrices no vinculantes, así como por la adopción de normas que pudieran estructurarse bajo un formato de protocolos o convenios internacionales, multilaterales y jurídicamente vinculantes.

28. Ambas metodologías debieran tomar en cuenta criterios básicos, como la injerencia no autorizada o la utilización ilícita de sistemas de información y telecomunicaciones y de recursos de información; los aspectos de soberanía asociados a estos temas; el uso pacífico de los medios de información y telecomunicaciones en todos sus aspectos; el fomento de la cooperación internacional con el objetivo de potenciar el desarrollo de los sistemas de información y telecomunicaciones en los países en desarrollo, a partir del impacto decisivo de las tecnologías de la información y las comunicaciones en el desarrollo socioeconómico; la prevención, enfrentamiento y erradicación de prácticas hostiles en el empleo de estos sistemas y la aplicación de medidas nacionales que establezcan un mayor control de los Estados sobre los sistemas de información y telecomunicaciones y enfrenten los actos delictivos correspondientes.

29. En adición a los elementos ya esbozados, Cuba considera necesario llamar la atención sobre los siguientes aspectos, estrechamente asociados a una plena potenciación de las telecomunicaciones como instrumento de fortalecimiento de la paz y la seguridad internacionales:

– 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.

– 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.

– Debe potenciarse la cooperación internacional en la materia, movilizando los recursos necesarios para asistir a los países en desarrollo en el fortalecimiento y expansión de sus sistemas de telecomunicaciones.

– Deben adoptarse medidas legislativas y de otra índole, tanto a nivel nacional como internacional, con el objetivo de prohibir la indebida concentración en

manos de privados 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.

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

– 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, poniéndose fin a las violaciones a la privacidad, a la soberanía y a la seguridad de muchos Estados, que llevan a cabo los sistemas globales de espionaje desarrollados por algunas potencias industrializadas y, en particular, los Estados Unidos.

– Desarrollo de garantías firmes de respeto a la diversidad cultural, que permitan eliminar toda forma de discriminación o incitación al odio en el contenido de la información difundida en los sistemas de telecomunicaciones a nivel internacional.

El Salvador

[Original: español]
[30 de junio de 2003]

Respuesta del Gobierno de El Salvador a la resolución 57/53 “los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional”, párrafo dispositivo 3

1. El Artículo 24 de la Constitución de la República prohíbe la interferencia y la intervención de las comunicaciones telefónicas, siendo éste el marco constitucional que actualmente impera en El Salvador en lo concerniente a la seguridad de la información y las telecomunicaciones;

2. En tal sentido, los Artículos 184, 185, 186 y 302 del Código Penal sancionan el apoderamiento de comunicación escrita, soporte informático o cualquier otro documento o efecto personal que no le esté dirigido o el apoderamiento de datos reservados de carácter personal o familiar; actos que implique captación de comunicaciones, como son interceptación o interrupción de comunicación telegráfica o telefónica y su interferencia e intervención, usando artificios técnicos de escucha o grabación de dichas comunicaciones.

3. Tales casos no son constitutivos de delitos, cuando se está recibiendo amenazas, exigiendo rescate de una persona que estuviere privada de libertad o secuestrada o se trate de delitos de crimen organizado y la víctima, el ofendido o su representante, en su caso, solicitaren o permitieren por escrito a la Fiscalía General de la República, la escucha y grabación de las conversaciones o acciones en que se reciban tales amenazas o exigencias.

4. La aplicabilidad del marco regulatorio de las telecomunicaciones y la imposición de sanciones administrativas, es competencia de la Superintendencia General de Electricidad y Telecomunicaciones, de acuerdo al artículo 4 de su Ley de Creación y artículo 29 literal (b) de la Ley de Telecomunicaciones, que indican la protección al secreto de las comunicaciones.

5. Durante los años 2001 y 2002, se impulsó ante la Asamblea Legislativa, una propuesta de reforma a la Constitución de la República, para que se permita la injerencia y/o intervención telefónica, como un mecanismo coadyuvante al combate del crimen organizado y la narcoactividad, misma que a la fecha aún no ha sido aprobada.

Federación de Rusia

[Original: ruso]
[28 de abril de 2003]

Cuestiones relacionadas con la labor del grupo de expertos gubernamentales encargados de estudiar el problema de la seguridad de la información

1. De conformidad con las resoluciones 56/19, de 29 de noviembre de 2001, y 57/53, de 22 de noviembre de 2002, tituladas “Los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional”, aprobadas por consenso por la Asamblea General de las Naciones Unidas, en 2004 se establecerá un grupo de expertos gubernamentales. En dichas resoluciones se encomienda al grupo de expertos gubernamentales que examine los peligros reales y potenciales en la esfera de la seguridad de la información, y las posibles medidas de cooperación para reducirlos, que prepare un estudio sobre los conceptos internacionales pertinentes encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones, y que presente un informe sobre los resultados de dicho estudio a la Asamblea General de las Naciones Unidas en su sexagésimo período de sesiones.

2. La Federación de Rusia toma nota de la importancia permanente y la actualidad cada vez más marcada del tema de la seguridad de la información internacional y considera que actualmente la seguridad de la información es un aspecto importante de la seguridad nacional de los Estados, así como parte del sistema común de seguridad internacional y estabilidad estratégica. Las cuestiones de la utilización de la tecnología y los recursos de la información y las telecomunicaciones guardan relación directa con la garantía militar y política de la seguridad de los países del mundo entero y, en consecuencia, exigen un enfoque mundial, amplio y no discriminatorio sobre la base de la participación del mayor número posible de países en el examen de dicha cuestión y el principio de la distribución geográfica equitativa.

3. Precisamente dicho enfoque permite garantizar la labor que se realice bajo el patrocinio de las Naciones Unidas, cuyo potencial como organización internacional fundamental representa más cabalmente los intereses de todos los países, y desempeña una función coordinadora en la esfera del desarme y permite establecer sobre su base un sistema equilibrado y eficaz de seguridad mundial.

4. Consideramos que en lo que atañe al estudio de toda la variedad de cuestiones relacionadas con la problemática de la seguridad de la información internacional, y también la elaboración de las recomendaciones pertinentes, han hecho un aporte útil

las resoluciones de la Asamblea General de las Naciones Unidas 53/70, de 4 de diciembre de 1998; 54/49, de 1° de diciembre de 1999; 55/28, de 20 de noviembre de 2000; 56/19, de 29 de noviembre de 2001, y 57/53, de 22 de noviembre de 2002, que tradicionalmente se han venido aprobando por consenso y que, en consecuencia, reflejan los pareceres sobre el problema en cuestión de toda la comunidad internacional, como asimismo las respuestas pertinentes de los Estados sobre el problema de la seguridad de la información que figuran en los informes del Secretario General de las Naciones Unidas A/54/213, A/55/140 y Corr.1 y Add.1, A/56/164 y Add.1 y A/57/166 y Add.1.

5. En lo que se refiere a dilucidar los enfoques existentes en la actualidad en relación con los problemas de la seguridad de la información internacional, hizo un importante aporte el seminario internacional sobre los problemas de la seguridad de la información internacional, organizado por el Instituto de las Naciones Unidas de Investigación sobre el Desarme y el Departamento de Asuntos de Desarme de la Secretaría de las Naciones Unidas y celebrado en agosto de 1999 en Ginebra, de conformidad con las recomendaciones de la resolución 53/70, en cuyo seminario participaron representantes de más de 50 países.

6. En el seminario se reafirmó lo acucioso que era el problema de la seguridad de la información y lo oportuno de plantear esta cuestión en el plano internacional, y también se logró distinguir los distintos enfoques al examen del fondo del problema. Actualmente no existen normas ni instrumentos internacionales de aceptación general y adecuados con arreglo a los cuales se pudieran examinar las cuestiones de la seguridad de información desde el punto de vista de las medidas para aminorar los peligros reales y potenciales en esta esfera a escala mundial.

7. A este respecto, resulta necesario estudiar en conjunto, con la participación lo más completa posible de los países, los conceptos y enfoques existentes a este respecto y también realizar un análisis de los instrumentos de derecho internacional existentes en este ámbito conforme a los distintos aspectos de la seguridad de la información internacional.

8. Consideramos que el examen multilateral internacional de dicha problemática está entrando a una etapa cualitativamente nueva, relacionada con el establecimiento de un grupo de expertos gubernamentales encargado de estudiar el problema de la seguridad de la información. El grupo de expertos gubernamentales otorga a la comunidad mundial una oportunidad única de estudiar toda la variedad de cuestiones susodichas.

9. La Federación de Rusia desearía participar constructivamente en la labor del grupo de expertos gubernamentales y, a este respecto, desearía expresar ciertas consideraciones relativas a las cuestiones que, a su juicio, podrían constituir el programa de su labor.

10. Al examinarse el problema de la seguridad de la información internacional se exige antes que nada partir de valores comunes a la humanidad como el de la garantía de intercambio internacional de la información universal libre, equitativo y seguro sobre la base de normas y principios del derecho internacional generalmente reconocidos.

11. Durante la labor del grupo en cuestión sería necesario tener en cuenta los aportes de los Estados recibidos de conformidad con las consabidas resoluciones de la Asamblea General de las Naciones Unidas sobre la seguridad de la información

internacional y otros materiales que se podrían presentar a la consideración de los miembros del grupo.

12. Según nuestro parecer, el grupo podría concentrar su examen en los siguientes aspectos, de importancia decisiva a nuestro juicio.

13. En primer lugar, convenir en el correspondiente mecanismo conceptual en la esfera de la seguridad de la información internacional. Podrían constituir importantes tareas de la primera etapa de la actividad del grupo de expertos gubernamentales la elaboración de definiciones básicas fundamentales: redes, recursos y sistemas de información, infraestructura informática, armas informáticas, y también la dilucidación del carácter, los indicios, la tipología y la clasificación de las amenazas a la seguridad de la información internacional.

14. En segundo lugar, examinar los factores que influyen sobre el estado de la seguridad de la información internacional. La seguridad de la información constituye una esfera compleja y variada, que exige por parte de la comunidad internacional un enfoque amplio que tenga en cuenta la existencia de amenazas tanto de carácter terrorista o delictivo como de carácter militar, tanto en la esfera militar como en la civil.

15. En la sociedad mundial de la información que se está configurando las tecnologías de la información y las comunicaciones están relacionadas entre sí y gozan de la propiedad de la transparencia. En consecuencia, en el marco de la sociedad mundial de la información la seguridad de la información internacional resulta estar vinculada indisoluble y naturalmente a las cuestiones de la determinación de la procedencia de las amenazas sobre aquélla de carácter interno o externo, las cuestiones de la soberanía nacional de los Estados y las cuestiones del respeto a los derechos y las libertades humanos, en particular el derecho a la no injerencia en la vida privada. Estas cuestiones y las cuestiones afines podrían dar pie para su examen durante la labor del grupo de expertos gubernamentales.

16. La siguiente etapa podría consistir en la determinación de medidas aceptables para todas las partes para prevenir la utilización de la tecnología y los medios de información para fines terroristas o fines delictivos de otra índole, así como medidas para limitar la utilización del arma de la información, sobre todo en relación con estructuras estatales de importancia crítica. Las tareas que deberían realizarse en dicha etapa, a nuestro juicio, serían el examen de la posibilidad de elaborar procedimientos de notificación mutua; la prevención de influencias de información transfronterizas no autorizadas; la creación de un sistema de supervisión internacional para detectar las amenazas que se manifiesten en la esfera de la información y un mecanismo de verificación del cumplimiento de las condiciones del régimen de seguridad de la información internacional, al igual que un mecanismo de resolución de situaciones conflictivas en la esfera de la seguridad de información, y las condiciones para crear un sistema internacional de certificación de tecnologías y medios informáticos y de telecomunicaciones (incluidos los programas lógicos) como parte de la garantía de su seguridad de información.

17. Convendría reflexionar sobre los posibles medios de interacción internacional de los órganos encargados de hacer cumplir la ley para prevenir y reprimir las transgresiones en el espacio informático, en particular, la dilucidación de la procedencia de agresiones informáticas; y echar una mirada al problema de la concordancia de las legislaciones nacionales de los distintos Estados que en parte reglamenten las

cuestiones de la seguridad de la información a fin de garantizar una tipificación unificada de las transgresiones en la esfera de la seguridad de la información y la responsabilidad en que se pueda incurrir en relación con la comisión de actos tipificados como delictivos.

18. También se propondría evaluar la posibilidad de prestar asistencia internacional a los países que resulten víctimas de ataques informáticos, con el fin de aminorar las consecuencias de los atentados al funcionamiento normal, sobre todo de instalaciones de infraestructuras críticas de los Estados.

19. En el futuro posiblemente podría tenderse a la elaboración de un instrumento de derecho internacional multilateral y aceptable para todas las partes, encaminado a fortalecer el régimen de la seguridad con arreglo al derecho internacional, de conformidad con el cual los Estados y otros sujetos del derecho internacional deberían asumir la responsabilidad internacional de las actividades en el espacio informático realizadas por ellos o desde un territorio que se halle bajo su jurisdicción.

20. La idea básica de la creación de un régimen universal de seguridad de la información internacional, a juicio de la Federación de Rusia, podría ser la obligación de los participantes de no recurrir a actos en el espacio informático cuyo fin sea causar perjuicios en las redes, los sistemas, los recursos y los procesos informáticos de otros Estados, su infraestructura, subversiones de los sistemas político, económico y social y el tratamiento sicológico masivo de la población con el fin de desestabilizar a la sociedad y al Estado.

Georgia

[Original: inglés]
[24 de junio de 2003]

1. El Gobierno de Georgia está en proceso de crear una estrategia de información nacional destinada al fomento de la esfera de las telecomunicaciones y la promoción de nuevas tecnologías, subrayando al mismo tiempo la importancia de la política estatal para garantizar la utilización de las tecnologías de la información.

2. Además, el Gobierno de Georgia está adoptando políticas tendientes a la integración de Georgia en la sociedad mundial de la información, siempre consciente de todos los riesgos y problemas que existen en lo que atañe a la seguridad de la información.

3. El Gobierno de Georgia estima sumamente importante participar en los programas y proyectos de cooperación internacionales destinados a establecer una sociedad internacional de la información más segura, en el entendido de que, habida cuenta de las realidades actuales de las tecnologías y los sistemas de información, al igual que de las peculiaridades de la región en que se encuentra Georgia, es imposible tratar unilateralmente las cuestiones de la seguridad de la información.

Senegal

[Original: francés]
[9 de junio de 2003]

1. Las medidas relativas a la seguridad de la información tienen lugar en la esfera del intercambio de información, en particular las vinculadas al tráfico de armas. Esas informaciones deben llevar el sello de la confidencialidad.

2. En consecuencia, deben estar garantizadas por cierto número de disposiciones, a saber:

- La seguridad de los equipos, los programas lógicos y los procesamientos de información mediante la instalación de dispositivos técnicos adecuados;
- La seguridad de los procedimientos de intercambio de información gracias a una reglamentación precisa y única.

Ucrania

[Original: ruso]
[27 de mayo de 2003]

1. Evaluación general de los problemas de la seguridad de la información

1. Los procesos internacionales de globalización, la implantación de las más modernas tecnologías de la información y la creación de una sociedad de la información refuerzan la importancia de un constituyente de la seguridad nacional como lo es la seguridad de la información.

2. El desarrollo de la infraestructura de información de un Estado y la creación e implantación de nuevas tecnologías de la información suscitan la aparición de ciertas amenazas a la seguridad de la información. Las más importantes de éstas son amenazas intencionales, que podrían estar motivadas por diferencias objetivas y subjetivas de intereses espirituales, intelectuales y materiales de los sujetos de las relaciones de información, así como medios, formas y métodos para satisfacerlos, lo que en conjunto puede llegar a ser la causa de una situación conflictiva.

3. Entre las principales amenazas a la seguridad de la información se cuentan:

- Manipulación de la información (desinformación, ocultamiento o tergiversación de la información);
- Violación del régimen establecido de intercambio de información, acceso no autorizado a los recursos de información o limitación injustificada de dicho acceso, recolección y utilización ilícitas de la información;
- Violación del espacio informático de un Estado o su utilización en intereses contrarios al Estado;
- Terrorismo informático; por ejemplo propagación de virus informáticos, instalación de dispositivos perturbadores lógicos y físicos, implantación de sistemas radioelectrónicos de intercepción de información en los medios técnicos y las viviendas, utilización ilícita de sistemas de información y telecomunicaciones o de recursos informáticos, implantación de información falsa, etc.;

4. Un resultado inmediato de las influencias negativas sobre la información es el desfiguramiento de la información, lo que conduce a la deformación o destrucción de los medios de información de un Estado y sus recursos informáticos, la imposibilidad del funcionamiento de importantes sistemas estatales, productivos, financieros, científicos y del patrimonio general y, en consecuencia, a la pérdida de la soberanía informática nacional.

5. De esta forma, el análisis de los problemas de la seguridad de la información demuestra que lo más común es que se relacionen con el problema del mantenimiento del volumen y la calidad necesarios de los recursos informáticos, la elaboración de estrategias para su utilización y la de las correspondientes tecnologías de la información, la creación de una infraestructura de información adecuada, la conservación de la seguridad de la información en los sistemas de información y telecomunicaciones, así como la lucha contra las influencias informáticas negativas sobre la persona, la sociedad y el Estado en conjunto.

6. Un grado insuficiente de protección de los recursos informáticos de un Estado puede llevar a apreciables perjuicios económicos a raíz de la desvalorización y la pérdida de sus componentes comerciales —tecnologías industriales y de información—, así como a atentados apreciables a la seguridad nacional en su conjunto como consecuencia de las posibles violaciones del funcionamiento normal de los sistemas de comunicaciones, control y dirección; la fuga de información que constituye secreto de Estado, etc.

7. La seguridad de la información supone la ejecución de medidas para proteger la información en todas las etapas en que se trabaja con ésta. El objetivo de la seguridad de la información consiste en garantizar la integridad de los sistemas, proteger y garantizar la precisión e integridad de la información, así como reducir a un mínimo las consecuencias que se puedan derivar en caso de que la información se modifique o destruya.

8. Una realidad objetiva del mundo contemporáneo es la utilización, en distintas esferas de la actividad vital de la sociedad y el Estado, de sistemas de información locales y mundiales destinados a acelerar el intercambio de la información y el acceso a los variados recursos de la información.

9. Una implantación extendida de dichos sistemas, en particular en aquellas esferas de actividad relacionadas con la administración estatal, crea oportunidades reales para un acceso no autorizado a los recursos de información de un Estado y los sistemas de gestión de aquéllos, la divulgación de comunicaciones de contenido ilícito, la vulneración de la integridad y la accesibilidad de la información, etc.

10. La estabilidad del funcionamiento de las esferas política, económica, militar, crediticio-financiera y de otra índole de un Estado depende no solamente de la eficacia, sino también de la solidez del funcionamiento de los sistemas de telecomunicaciones e información. En condiciones de la creación de un espacio informático, resultan especialmente acuciosas y candentes las cuestiones de la solidez y la protección de los sistemas de información y telecomunicaciones que funcionan en interés de la administración del Estado. Al tener acceso a los sistemas de información, no sólo se puede obtener información importante, sino que, mediante la interrupción o el bloqueo del funcionamiento de los sistemas de información se puede paralizar total o parcialmente la actividad de empresas de importancia vital e incluso sectores

enteros de la economía, ejercer influencia negativa sobre los recursos de información y divulgar información en contra de las prohibiciones legislativas, etc.

11. La garantía de la seguridad de la información que circula en las redes de información y telecomunicaciones es uno de los factores principales y una condición necesaria de la garantía de la seguridad de la información, la soberanía nacional y estatal y el desarrollo sostenible de la sociedad.

12. En la presente etapa del desarrollo de los sistemas de información y telecomunicaciones las amenazas más importantes a la información que circula en aquéllos son:

– La violación del régimen de plantilla del funcionamiento de importantes sistemas de información y telecomunicaciones;

– Acciones casuales o intencionadas que provocan violaciones de la confidencialidad, la integridad y la accesibilidad de la información;

– Exacerbación de la situación de enfrentamiento de la información (propagación de virus informáticos, instalación de dispositivos físicos y lógicos perturbadores, instauración de dispositivos electrónicos para la intercepción de información en recursos e instalaciones técnicas, intercepción y desciframiento de información, implantación de información falsa, influencias radioelectrónicas en sistemas de contraseñas y claves, aniquilamiento radioelectrónico de las líneas de comunicaciones y los sistemas de control, etc.).

13. Sólo se puede asegurar la protección firme de los sistemas de información y telecomunicaciones, sobre todo de los órganos de la administración estatal, contra atentados criminales, mediante la implantación de un sistema complejo de protección de la información, que incluya la utilización de medios criptográficos y técnicos de protección, así como la ejecución de una serie de medidas de organización y técnicas.

14. Se debe prestar especial atención al problema de la conexión de redes de computación a las redes informáticas internacionales.

15. El ingreso de Ucrania de pleno derecho en la comunidad internacional es imposible si no se amplían las interacciones con las redes informáticas mundiales de transmisión de datos como la Internet. Dichos sistemas proporcionan un gran surtido de servicios modernos de información y telecomunicaciones, muchos de los cuales se publicitan como sistemas que garantizan la protección de la información.

16. Al mismo tiempo, un gran número de medios que se utilizan en dichos sistemas, cuyas propiedades especiales, en ausencia de los manuales de programas iniciales, son muy difíciles de evaluar, o incluso imposibles, constituyen una amenaza a la seguridad de la información, las transacciones financieras y los pagos electrónicos. Son conocidos los numerosos ejemplos de utilización irreflexiva por los bancos de tecnologías de información importada, que permiten a un especialista entrometerse en un sistema durante una sesión de 10 minutos de comunicaciones.

17. Es necesario prestar atención al peligro de la conexión irreflexiva a las redes mundiales de centros de suscripción y a las redes locales. Prácticamente cualquier red informática local que se conecte a la Internet sin utilizar las medidas pertinentes de protección resulta fácilmente accesible a los piratas cibernéticos o “hackers”.

18. La transición a nuevas formas y métodos de ejecución de las relaciones sociales informáticas y, en particular, la amplia divulgación de nuevas formas de actividad empresarial que utilizan la red de la Internet (comercio electrónico), así como la instauración gradual de sistema de administración electrónica, está acompañada por la amplia utilización de la tecnología informática y el aumento de los volúmenes de información en forma electrónica. Esto ocasiona una dependencia cada vez mayor de los sujetos de las relaciones de información con respecto al grado de protección de dicha información, la cual, a su vez, atrae la atención de elementos de la sociedad con intenciones negativas y sus agrupaciones. La inadecuación de los sistemas y mecanismos de protección existentes conduce a que se configuren condiciones reales para el acceso no autorizado, así como la utilización, el bloqueo o la destrucción de información que se crea, se elabora, se transmite y se conserva en forma electrónica.

19. En resumen, el problema de la injerencia en los recursos de información de los Estados es una cuestión acuciante para el mundo entero. Si hasta principios del decenio de 1990 la cuestión más acuciosa era la protección de un Estado contra el espionaje extranjero, en este último tiempo, en lo que se refiere a la amplia instauración de tecnologías de información en todas las esferas de la vida social, ha pasado a primer plano el problema de la lucha contra los llamados delitos informáticos. De esto puede dar testimonio el hecho de que los delitos informáticos son reconocidos en el plano internacional como una nueva forma de delitos intelectuales. A ese respecto, los delitos en esta esfera no sólo son cometidos por grupos de la delincuencia organizada, sino también por terroristas y transgresores aislados.

20. Son más atractivos para los delincuentes los sistemas de información de los órganos de la autoridad estatal, los órganos encargados de hacer cumplir la ley, aduaneros y fiscales, las instituciones crediticio-financieras, la esfera militar, etc. En particular, en Ucrania los órganos encargados de hacer cumplir la ley repetidamente han detectado operaciones ilícitas relacionadas con la utilización de tarjetas de crédito y débito de los sistemas de pagos internacionales, así como la ejecución de pagos electrónicos ficticios con el objeto de obtener dinero en forma ilegítima, la injerencia en el funcionamiento de redes de computación mediante la Internet, etc.

2. 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 información o la utilización ilícita de esos sistemas

21. En condiciones de desarrollo impetuoso de las tecnologías de la información y las telecomunicaciones, se torna acuciante el problema de garantizar la seguridad de la información, en particular la solución de los problemas de la injerencia no autorizada o la utilización ilícita de los sistemas de información y telecomunicaciones, así como la protección de los recursos de información.

22. A este respecto, por la noción de “seguridad de la información” debe entenderse una situación de protección del espacio informático de un Estado tal que se satisfacen los intereses nacionales y se respetan los derechos de la persona, la sociedad y el Estado.

23. Habida cuenta del gran peligro para la sociedad de los actos ilícitos antes mencionados y prestando atención a la importancia de un funcionamiento eficaz de los sistemas de información y telecomunicaciones, en el Código Penal de Ucrania se tipifican delitos en la esfera de la utilización de los ordenadores electrónicos

(computadoras), los sistemas y las redes de computación y se prevén las correspondientes sanciones por la comisión de dichos delitos, en particular:

– Injerencia ilícita en el funcionamiento de ordenadores electrónicos (computadoras), sistemas y redes de computación —actos que conduzcan a la tergiversación o la destrucción de información computadorizada o los portadores de esa información—, así como la propagación de virus informáticos mediante la utilización de medios lógicos y físicos, destinados a la penetración ilícita en dichas máquinas, sistemas y redes de computación;

– Robo, usurpación o exacción de información computadorizada o apoderamiento de esta última mediante engaño o uso indebido de la posición como empleado;

– Violación de las normas de explotación de las computadoras automatizadas, sus sistemas o redes de computadoras por una persona responsable de su explotación y funcionamiento, que pueda ser causa del robo, la tergiversación o la destrucción de información computarizada o los medios para su protección, la copia ilícita de información computadorizada o un daño apreciable al funcionamiento de dichas máquinas, sus sistemas o redes de computación.

24. Generalizando, la noción "transgresión informática" puede definirse como una acción ilícita que atenta contra el régimen establecido del funcionamiento de sistemas de información y el régimen de acceso a dichos sistemas y vulnera la integridad, la confidencialidad o la accesibilidad de la información y los derechos y libertades de los ciudadanos durante la actividad informática.

3. Contenido de los conceptos internacionales encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones

25. El siglo XXI debe pasar a la historia como el período de establecimiento y desarrollo de la sociedad mundial de la información, que sustituye o complementa los procesos materiales con procesos informáticos y también contribuirá a un aumento considerable de la productividad del trabajo y al mejoramiento del bienestar social. Muchos países ya están creando la base de organización y técnica para la infraestructura nacional y mundial. Las Naciones Unidas están examinando la cuestión de introducir el derecho al acceso a los sistemas básicos de comunicaciones e información en la Declaración Universal de Derechos Humanos.

26. La experiencia de los países desarrollados en relación con una solución efectiva del problema de la informatización en la segunda mitad del decenio de 1990, generalizada por organizaciones internacionales (Unión Internacional de Telecomunicaciones, Organización Internacional de Normalización/Comisión Electrotécnica Internacional e Instituto Europeo de Normas de Telecomunicación) y numerosas organizaciones nacionales de normalización convence de la necesidad de la creación de infraestructuras de información en múltiples planos (nacionales y regionales) con una posterior adhesión a la infraestructura mundial de la información (GII).

27. La participación de Europa en la GII no sólo entraña la creación de una infraestructura europea de la información (EII) en el marco de la región, sino también la cooperación en la construcción de infraestructuras nacionales de información en los distintos países para lograr ventajas recíprocas para cada país y para Europa en general. Junto con la utilización del término EII los europeos otorgan prioridad a la utilización de la noción "Sociedad europea de la información" (EIS). Los bloques

constructivos de la EIS son las redes, los servicios básicos y los accesorios. Las redes existentes en Europa pueden reforzarse mediante la realización de una supertroncal europea de banda ancha, que aúne en un todo único las redes europeas de telecomunicaciones, cable y satélite. Los países de Europa apoyan la utilización de servicios básicos transeuropeos, incluidos los servicios de correo electrónico, transmisión de datos y vídeo.

28. Los países europeos también prestan gran atención al aspecto social de la actual etapa de la revolución tecnológica mundial. Hay resoluciones y documentos del Consejo de Europa dedicados a la formulación de una política nacional en la esfera de la construcción de una sociedad de la información. A este respecto, las tareas antes mencionadas no se perciben como un tributo a la moda, sino como condiciones necesarias de desarrollo, cuya omisión da lugar a la pérdida de las tasas de crecimiento y el retiro de posiciones económicas y tecnológicas de vanguardia.

29. Las tendencias mundiales de la reglamentación jurídica de la actividad en la esfera de las más modernas tecnologías de transmisión de datos dan testimonio de la necesidad de elaborar enfoques unificados para la creación de instrumentos legislativos y normativos para todos los participantes en el intercambio internacional de información. Según una conclusión de la Asociación Americana de Juristas, actualmente existe una real necesidad de crear una comisión multinacional de legislación sobre el ciberespacio. Dentro de la lista de decisiones cuyo examen se recomienda a la futura comisión, una de las más importantes es la creación de un cibertribunal. En las condiciones actuales el problema principal de la garantía jurídica de la seguridad de la información es la necesidad de insertar las normas jurídicas existentes de conformidad con los avances en la tecnología de la información.

30. Hoy en día es imposible imaginar un espacio informático sin redes de computación. Precisamente estas tecnologías dieron impulso a la aparición y el desarrollo de muchas formas de negocios: tarjetas electrónicas de débito y crédito, cuentas interbancarias operativas, servicios bursátiles, escritorios de intermediarios, etc.

31. Se espera que para 2005 la mitad de la población de la Unión Europea (UE) tendrá acceso a la Internet. Por esta razón los países de la UE encaminan sus esfuerzos al fomento de la confianza en las operaciones comerciales y financieras por conducto de la Internet y también a la transición acelerada al comercio electrónico.

32. El Parlamento Europeo aprobó el 7 de mayo de 1999 el proyecto de ley ENFOPOL 98, que da derecho a los órganos competentes a realizar la supervisión de redes en forma legal. El proyecto de ley se presenta como proyecto de resolución del Consejo de la UE “sobre la supervisión legal de las telecomunicaciones habida cuenta de las nuevas tecnologías”. El documento insta a que se hagan accesibles para los órganos que realizarán la vigilancia en tiempo real todas las redes de telecomunicaciones, inclusive la Internet y los sistemas satelitales de comunicaciones telefónicas. Por su parte, el Gobierno del Reino Unido ha iniciado la ejecución de un proyecto de creación de un centro que se ocupará de la intercepción de todo el tráfico electrónico al interior del país.

33. El Gobierno de China, para efectuar la fiscalización del acceso a una red, lo hace mediante la concesión de licencias para la utilización de módems, y todas las corrientes de información de la Internet se encaminan a través de un número limitado de explotadores nacionales.

34. Entre los problemas de la seguridad de la información cabe distinguir los siguientes:

– Violación de los derechos de propiedad intelectual;

– Divulgación de información que influye negativamente sobre la salud social de las personas, inclusive los problemas relacionados con el acceso de los niños a la Internet;

– Realización de operaciones comerciales ilícitas;

– Acceso no autorizado a información confidencial;

– Violación de los derechos e intereses legítimos de las personas durante el intercambio de información;

– Difusión de avisos publicitarios de mala calidad.

35. Existe otro peligro más de la Internet, que consiste en la posibilidad de utilizar información confidencial de una persona sin su consentimiento. Es posible reunir dichos datos analizando la información de que disfruta una persona en la Internet.

36. La Internet es un medio muy especial de comunicación y, a consecuencia de su carácter transfronterizo, difícilmente se presta a la reglamentación jurídica. Todos los participantes en la Internet están sujetos a las leyes vigentes en sus países. Al mismo tiempo, un contenido ilícito puede manifestarse fuera del territorio del país donde se conserva en un servidor. A este respecto, para la reglamentación de las relaciones jurídicas en la Internet hacen falta convenios internacionales, cuya adopción a su vez se complica debido a los distintos enfoques de la legislación de los Estados a una u otra transgresión; por ejemplo, se atribuyen distintos significados a la noción de "pornografía". Actualmente la orientación más general de las iniciativas legislativas en la esfera de la Internet está encaminada al establecimiento de la responsabilidad de los proveedores de servicios de huésped del contenido de la información que figura en sus computadoras. Puesto que esto resulta muy complejo desde el punto de vista técnico, en la legislación de varios países la responsabilidad de los proveedores está condicionada a que supieran del contenido de la información ilícita.

37. La Organización Internacional de la Policía Criminal (Interpol), que reúne a los órganos encargados de hacer cumplir la ley de 178 países del mundo, comunicó que emplazará información sobre delitos en redes en el sitio de la empresa estadounidense Atomic Tangerine. La Interpol proporciona información sobre los piratas cibernéticos, y también sobre las formas de delitos que amenazan a las empresas que se ocupan de negocios electrónicos. Por su parte, Atomic Tangerine debe proporcionar a la Interpol la información recibida con la ayuda del sistema de alerta temprana NetRadar, que pertenece a la empresa y está destinado a realizar vigilancia en la Red.

38. Uno de los problemas importantes es el del anonimato de las comunicaciones, que complica, y a veces incluso hace imposible, el establecer quién es la persona poseedora de información ilícita, y también llamarla a rendir cuenta. Por esta razón los expertos de muchos países proponen reforzar en el plano legislativo la prohibición de comunicaciones anónimas habiéndose autorizado a este respecto las comunicaciones bajo seudónimos, para los cuales en caso de necesidad podría establecerse quién es el autor.

39. El 21 de diciembre de 1998 el Consejo de la UE aprobó el plan de acción propuesto por el Parlamento Europeo para la seguridad en la utilización de la Internet. El plan tenía una vigencia de cuatro años (del 1° de enero de 1999 al 31 de diciembre de 2002). Su presupuesto ascendió a 25 millones de euros. Conforme al plan, se proponía la creación de distintos "niveles de calidad" de la Internet, que debían constituirse de conformidad con los "indicadores de calidad de la Internet" de producción. Estas disposiciones debían reforzarse tanto en las legislaciones nacionales como en los códigos de autorreglamentación de los proveedores de servicios en la Internet. En marzo de 1999, la Comisión Europea, conforme a los resultados del examen de las disposiciones del informe sobre la convergencia de las telecomunicaciones, los medios de información de masas y la tecnología de información, aprobó un informe cuya conclusión fundamental en particular era la siguiente afirmación: la reglamentación jurídica de la Internet debe tener un carácter transparente, claro y proporcionado.