Naciones Unidas A/57/166/Add.1

Asamblea General

Distr. general
29 de agosto de 2002
Español
Original: árabe/español/inglés

Quincuagésimo séptimo período de sesiones
Tema 62 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**

Adición

Índice

* A/57/150.
** La información que figura en el presente documento se recibió tras la presentación del informe principal.

02-56152 (S) 230902 230902

Respuestas recibidas de Gobiernos

[Original: español]
[15 de julio de 2002]

Cuba

Evaluación general de los problemas de la seguridad de la información

1. Es inmenso el desarrollo científico-tecnológico experimentado por la humanidad en las últimas décadas. Sin duda los avances logrados en la informática y las telecomunicaciones han constituido una revolución tecnológica que alcanza toda la actividad humana. La combinación de la informática con el avance de las telecomunicaciones amplía las potencialidades de ambas ramas a límites inimaginables.

2. La introducción de ordenadores compactos de gran velocidad y capacidad de operación, la utilización de nuevos materiales que aumentan la velocidad de la transmisión de información y la proliferación de satélites de comunicación, son sólo algunos ejemplos de los logros obtenidos.

3. El proceso de globalización en curso es uno de los resultados palpables de la llamada revolución tecnológica. Las distancias se acortan y las comunicaciones y el flujo de información operan en tiempo real. Los procedimientos industriales han cambiado radicalmente, y las herramientas informáticas actúan aceleradamente en el rediseño de los procesos productivos, lográndose niveles de eficiencia nunca antes vistos.

4. Esas transformaciones abarcan no sólo al sector civil, sino también a la industria militar. Hoy la informática es componente indispensable de los armamentos modernos y sus sistemas. Hemos sido testigos, durante la última década, de diferentes conflictos armados donde se ha hecho alarde de sofisticados armamentos con un potencial destructivo y un nivel de precisión mortífera para atacar sus blancos nunca antes vistos, y que son resultado, en buena medida, de la aplicación de los avances informáticos.

5. Las herramientas informáticas han demostrado sus potencialidades. Por ejemplo, los software encuentran una amplia gama de aplicaciones, entre los que proliferan cada vez con mayor fuerza programas malignos o de efectos malignos de alto nivel destructivo que pueden lograr, en un tiempo relativamente corto, daños irreparables en cualquier lugar del mundo debido al incremento de las redes informáticas y los niveles de accesos a esas redes.

6. La dependencia que van creando estas tecnologías llama a la reflexión colectiva, con el objetivo de asegurar un uso adecuado de todos esos medios.

7. La propia inscripción del tema en el programa de la Asamblea General, demuestra que la comunidad internacional ha tomado conciencia de los potenciales peligros para la paz y la seguridad internacionales, cuando estas tecnologías no son utilizadas con fines pacíficos.

8. Por otra parte, el uso hostil de las telecomunicaciones en algunos casos, bajo el propósito declarado o encubierto de subvertir el ordenamiento jurídico y político de los Estados, es otra 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.

9. La resolución 56/19 de la Asamblea General nos brinda la oportunidad de analizar todos los aspectos de la información y las telecomunicaciones en el contexto de la seguridad internacional, entre los que se encuentra la posibilidad de reforzar y ampliar el derecho internacional vigente en esta materia.

Determinación de criterios básicos relativos a la seguridad de la información, en particular la injerencia no autorizada o la utilización ilícita de sistemas de información y telecomunicaciones y de recursos de información

10. Se relacionan algunos criterios esenciales.

1. La homologación de normas y procedimientos

11. La no existencia de un código de ética común para todos los usuarios, dada la voluntariedad de la asociación a las redes de Internet y el empleo de los satélites y otros medios de comunicaciones, pone en riesgo la seguridad de la información que por esos medios se tramita.

12. Exigencias tales como la *confidencialidad, integridad y disponibilidad* caracterizan a una red en su eficiencia de empleo. Estos aspectos garantizan que cada

información sea vista sólo por los usuarios autorizados, no sea modificada y se encuentre lista para acceder a ella cuando se le necesita.

13. Cuando no se respetan estas exigencias, disminuye o desaparece la seguridad. Cada productor de medios informáticos debe garantizar que su software o hardware no permita accesos ilegales, ni que se produzcan armas informáticas capaces de dañar a algunos de los elementos de los sistemas de información. En general, estos principios son validos para toda implementación de servicios o generación de productos, sistemas de tecnologías de información y comunicaciones.

14. Esto será posible en la medida en que cada productor de sistemas informáticos establezca mejores controles sobre los procesos de producción, las tecnologías y los sistemas, y además, mantenga un seguimiento, con iguales propósitos, en la explotación y el uso ulteriores de esos sistemas y tecnologías. Del mismo modo, son necesarios mecanismos de colaboración que permitan el aviso mutuo entre suministradores y usuarios de cualquier violación que se detecte y que determinen la responsabilidad de los productores ante la solución de los problemas de seguridad de los productos que comercializan.

15. Resulta necesario establecer los estándares mínimos para generar tecnología en un ambiente de seguridad, las cuales deben certificarse también, dado que favorecería los mecanismos de homologación. En este sentido, Cuba estaría dispuesta a colaborar con su modesta experiencia en este campo con aquellos países interesados.

2. Injerencia no autorizada en los sistemas de información o de telecomunicaciones

16. Deben fortalecerse las regulaciones internacionales que impidan agresiones a estos sistemas. Los Estados aisladamente no pueden enfrentar esta problemática. El nivel de interdependencia que establece la universalidad de las redes informáticas y los sistemas de telecomunicaciones hacen imposible que el asunto sea tarea de un solo Estado.

17. Deben respetarse las normas internacionales ya existentes. Los accesos a los sistemas de información o de telecomunicaciones de otro Estado sólo deben ocurrir previo consentimiento del Estado concernido, y en las formas y magnitudes que éste determine.

18. La seguridad y la paz internacionales pueden verse dañadas por la agresión a los sistemas de información o de telecomunicaciones de Estados ajenos. Estos procedimientos ya son utilizados como herramientas para la aplicación de políticas hostiles.

19. Cuba sufre ese tipo de agresiones promovidas, consentidas y ejecutadas por el Gobierno de los Estados Unidos de América. Para que sólo se tenga una idea de la gravedad del asunto, nuestro país durante varias décadas se ha visto sometido a la agresión radial y televisiva de los Estados Unidos con el declarado propósito de subvertir el orden interno y derrocar al Gobierno de la República de Cuba.

20. Para ello, por ejemplo, desde enero del 2001 hasta marzo del 2002 han transmitido, desde territorio de los Estados Unidos como promedio un total de 15 estaciones radiales y televisivas, con informaciones falsas y tendenciosas de claro contenido subversivo.

21. Esas estaciones han transmitido diariamente en ese período entre 312 y 319 horas de señales radiales por onda media, onda corta y frecuencia modulada. Como promedio, eso significa 2.257 horas semanales. Si le sumamos también las señales televisivas, se alcanzaría una cifra de 2.288 horas semanales en total.

22. En esa agresión radial y televisiva el Gobierno de los Estados Unidos ha invertido, desde 1990, más de 20 millones de dólares al año y específicamente en este año fiscal, alrededor de 24 millones de dólares.

23. En la mayoría de los casos, la información incita a la desobediencia civil y a la ejecución de actos vandálicos y terroristas. Incluso, en fecha reciente, una emisora radial del Gobierno de los Estados Unidos provocó un incidente dirigido a crear situaciones de desorden interno en Cuba y en donde, además, estuvo involucrada la representación diplomática de un tercer país, creando situaciones de tensión que habrían podido dañar las relaciones diplomáticas de Cuba con ese país.

3. Utilización ilícita de sistemas de información y telecomunicaciones

24. Se trata del empleo de estos sistemas al margen de los procedimientos y las normas acordadas internacionalmente y en contravención de las regulaciones nacionales correspondientes. Los Estados que aún no lo hayan hecho, deben adoptar todas las medidas necesarias para fortalecer dichas regulaciones nacionales.

25. Resulta 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.

26. En la actualidad, prácticamente ninguna esfera de la sociedad, ni ninguna actividad humana, escapa a la influencia de los sistemas de información o los sistemas de telecomunicaciones, haciendo que los efectos de la utilización inapropiada de esos medios sean incalculables.

4. Los sistemas de información y telecomunicaciones son tecnologías de doble uso

27. Una de las peculiaridades del desarrollo histórico en esta materia es que el surgimiento del empleo de nuevas tecnologías ha oscilado entre las aplicaciones civiles y militares. Es decir, muchas de las tecnologías que hoy se utilizan extensamente en la vida civil, tuvieron su origen en la rama militar, y viceversa.

28. Eso obliga a que los esfuerzos de la comunidad internacional en este tema deban orientarse en dos direcciones: la prevención, enfrentamiento y erradicación del empleo de los sistemas de información y telecomunicaciones para fines hostiles y la potenciación de la cooperación internacional en el empleo de los mismos pacíficamente.

29. Ello contemplaría, entre otros aspectos, el análisis de los siguientes elementos relacionados con los sistemas de información y telecomunicaciones:

a) El diseño y la aplicación universal de procedimientos que impidan los accesos no autorizados a los sistemas;

b) La transparencia en el empleo de esos medios;

c) La proyección de medidas específicas para la protección de sistemas informáticos vinculados a las armas de exterminio en masa y otros armamentos sofisticados;

d) La adopción de medidas para impedir los accesos no autorizados a los sistemas de información de centrales electronucleares, centrales eléctricas u otras instalaciones estratégicamente importantes para un país;

e) El intercambio de información entre los Estados sobre actividades ilícitas en que incurran personas naturales o jurídicas que se encuentren bajo su control o jurisdicción, guiados fundamentalmente por la voluntad de prevenir los actos ilícitos;

f) El incremento de la cooperación internacional encaminada a facilitar las transferencias de tecnologías y la formación o consolidación de las capacidades nacionales pertinentes;

g) La prohibición de la instalación de medios en el espacio ultraterrestres con fines militares;

h) Reforzar el principio básico de las relaciones internacionales referido a la no injerencia en los asuntos internos de los Estados, a través, entre otras, de la adopción de medidas que prohíban la utilización de los sistemas de información y telecomunicaciones para esos fines.

5. Armas de la información

30. Los sistemas de información y telecomunicaciones pueden convertirse en armas cuando se diseñan y/o se 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 a través de medios no autorizados o consentidos por el Estado agredido; la influencia en el comportamiento de las personas con el propósito de desestabilizar las sociedades, derrocar gobiernos o modificar el ordenamiento político y social de los países.

6. Terrorismo aplicado a los sistemas de información y telecomunicaciones

31. El terrorismo debe ser combatido y rechazado en todas sus formas y manifestaciones, provenga de quien provenga y hágase contra quien se haga. Estas tecnologías no están exentas de ser empleadas para acometer actos de terrorismo. Su amplia difusión, el relativo fácil acceso a las mismas, la relación costo-impacto de su empleo, hacen atractivas estas tecnologías para los terroristas.

32. Las acciones pudieran ser tan disímiles y tan peligrosas como la interrupción de los sistemas automatizados de los aeropuertos; la interferencia en los sistemas de navegación de los aviones comerciales; el daño a los sistemas de control de centrales eléctricas, fuentes de abasto de agua y viales para automóviles; daño a las redes de comunicación; entre otras.

33. Una evaluación de los avances de la información y las telecomunicaciones en el contexto de la seguridad internacional requiere ineludiblemente atender los problemas asociados al terrorismo. Quizás, una vía inmediata para abordar este asunto sean las negociaciones que se llevan a cabo en las Naciones Unidas sobre la lucha internacional contra el terrorismo para el establecimiento de normas y regulaciones internacionales, así como en otras iniciativas multilaterales pertinentes.

34. Cuba está dispuesta a analizar estos y otros criterios básicos que sean propuestos y considera que la Organización de las Naciones Unidas, como máximo garante de la paz y la seguridad internacionales, es el órgano idóneo para discutir estas cuestiones.

35. Además, deben ser involucradas en el debate las instituciones internacionales especializadas en los sistemas de información y telecomunicaciones.

Conveniencia de elaborar los principios internacionales que aumenten la seguridad de los sistemas de información y de telecomunicaciones mundiales y ayuden a luchar contra el terrorismo y la delincuencia en la esfera de la información

36. Resulta evidente la necesidad de fortalecer el derecho internacional en materia de información y telecomunicaciones. No se parte de la nada, ya existen principios, regulaciones y procedimientos internacionales afines que deben ser tornados en cuenta. Las experiencias nacionales también deben ser consideradas.

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

38. Ambas metodologías debieran afrontar los criterios básicos aquí esbozados y otros que sean propuestos, particularmente 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; la prevención, enfrentamiento y erradicación de prácticas hostiles en el empleo de estos sistemas; 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.

[Original: español]
[24 de junio de 2002]

Panamá

1. La República de Panamá reconoce el peligro que los grandes avances tecnológicos en la información y en las telecomunicaciones han convertido al denominado “campo de batalla virtual” en un nuevo desafío a la seguridad internacional: la tecnología incide no sólo en el conflicto armado en sí sino en su resolución (inteligencia, blancos, calidad versus cantidad de las armas).

2. La realización de un ataque utilizando las nuevas tecnologías de la información y de las telecomunicaciones puede provocar mayores daños que los que causaría, por ejemplo, un bombardeo convencional. Actualmente, las computadoras regulan la información financiera, el flujo de petróleo y gas por los oleoductos, las reservas de agua y el control de los embalses, el control del tráfico aéreo, el control de tránsito por el Canal de Panamá y los servicios de emergencia, entre otros. De allí que 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, requiere de sistemas de protección acorde con esta nueva expresión de violencia. Sin embargo, tales sistemas de protección (firewalls, etc.) demandan gran cantidad de recursos financieros y humanos, los cuales no son fáciles de lograr en muchos de nuestros países.

3. Así, el fortalecimiento de la seguridad de los sistemas mundiales de información y telecomunicaciones requiere del establecimiento de un sistema seguro que permita el intercambio de información con otros Estados con el fin de monitorear y prevenir actividades o comunicaciones de individuos o de redes de individuos que sí utilicen la tecnología de las comunicaciones para preparar sus actividades criminales. No obstante, esta necesidad se traduce en un compromiso y en una obligación por parte de los países tecnológicamente avanzados de proveer, transferir y capacitar a los que no lo son. Asimismo, estos países deben comprometerse a no utilizar su ventaja tecnológica en actividades de espionaje comercial o industrial en detrimento del resto de los países menos aventajados tecnológicamente.

4. A pesar de los daños que pueden causar, Internet y las nuevas tecnologías de la información y de las

telecomunicaciones son medios que adecuadamente utilizados pueden de hecho contribuir a la seguridad internacional al proveer las herramientas necesarias para la consecución del fin de la seguridad humana.

[Original: árabe]
[28 de agosto de 2002]

República Árabe Siria

A continuación, explicamos el punto de vista de las autoridades competentes de la República Árabe Siria sobre la cuestión de los avances en la esfera de la información y las comunicaciones alámbricas e inalámbricas en el contexto de la seguridad internacional:

- Es preciso levantar el embargo de tecnologías de información y comunicaciones y exportar esta tecnología a los Estados en desarrollo que son Miembros de las Naciones Unidas.
- Las Naciones Unidas deben desempeñar una función activa, desde el punto de vista legislativo y material, a la hora de salvar la brecha numérica que separa a los Estados avanzados desde el punto de vista tecnológico y científico de los Estados en desarrollo.
- Es preciso aprobar leyes que impidan a los Estados, organizaciones e individuos introducirse de forma ilegal en los sistemas de información y comunicaciones de otros Estados, y que estas leyes dispongan penas disuasorias contra las partes que las contravengan.
- Hay que aplicar las resoluciones aprobadas por la Unión Internacional de Telecomunicaciones (UIT), que protegen las áreas de frecuencia privativas de cada uno de los Estados Miembros de las Naciones Unidas frente a la distorsión o la interferencia ilegítima por otro Estado o entidad.
- Deben establecerse principios y normas internacionales para difundir datos específicos a la historia, la cultura y la civilización de los pueblos mediante bases y redes de datos (la Internet), evitando la falsificación de datos y adoptando contra los infractores las medidas convenientes y factibles.
- Es preciso crear una autoridad internacional de referencia, que goce de respaldo internacional y cuya tarea consista en presentar justificaciones y pruebas a los Estados que deban cooperar en materia de seguridad en lo relativo a sus sistemas de información y comunicaciones. Una de las tareas de esta autoridad internacional será ofrecer ayuda material y tecnológica a estos Estados, para permitirles que hagan realidad las mejoras que deban llevar a cabo, y también capacitar a un cuerpo técnico especializado de estos Estados sobre formas de cooperación mediante tecnologías de seguridad en relación con los sistemas de información y comunicaciones.