

**Asamblea General**

Distr. general  
10 de julio de 2000  
Español  
Original: árabe/inglés/ruso

**Quincuagésimo quinto 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**

|                                                      | <i>Página</i> |
|------------------------------------------------------|---------------|
| I.. Introducción . . . . .                           | 2             |
| II.. Respuestas recibidas de los gobiernos . . . . . | 2             |
| Federación de Rusia . . . . .                        | 2             |
| Jordania . . . . .                                   | 6             |
| Qatar . . . . .                                      | 7             |

\* A/55/150.

\*\* El presente informe se prepara con arreglo a la información enviada por los Estados Miembros.

## I. Introducción

1. La Asamblea General, en los párrafos dispositivos segundo y tercero de su resolución 54/49, de 1° de diciembre de 1999, sobre avances en la información y las telecomunicaciones en el contexto de la seguridad internacional, invitó a todos los Estados Miembros a que siguiesen haciendo llegar al Secretario General sus opiniones y observaciones sobre las cuestiones siguientes: a) evaluación general de los problemas de la seguridad de la información; b) 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 de telecomunicaciones y de recursos de información; c) conveniencia de elaborar 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, y pidió al Secretario General que le presentase un informe en su quincuagésimo quinto período de sesiones.

2. El 14 de marzo de 2000, el Secretario General dirigió una nota verbal a los Estados Miembros en la que les solicitaba que le ofreciesen sus puntos de vista, de conformidad con la invitación de la Asamblea. Las respuestas recibidas de los gobiernos hasta la fecha se reproducen en el capítulo II del presente informe. Cualesquiera otras respuestas recibidas serán publicadas como adición al presente informe.

## II. Respuestas recibidas de los gobiernos

### Federación de Rusia

[Original: ruso]  
[12 de mayo de 1999]

### Principios relativos a la seguridad internacional de la información

#### Empleo de términos

A los efectos de los presentes Principios se emplearán los siguientes términos:

1. **Esfera de la información:** esfera de actividad relacionada con la creación, transformación y utilización de la información, inclusive la conciencia individual y colectiva, la infraestructura de información y telecomunicaciones y la información propiamente tal.

2. **Recursos de información:** infraestructura de información (medios físicos y sistemas de creación, tratamiento, almacenamiento y transmisión de información), inclusive archivos y bases de datos y la información propiamente tal y sus corrientes.

3. **Guerra de información:** enfrentamiento entre Estados en la esfera de la información con objeto de provocar daños a los sistemas, procesos y recursos de información y a las estructuras de importancia crítica y socavar los sistemas político, económico y social, así como la manipulación psicológica masiva de la población con objeto de desestabilizar a una sociedad y un Estado.

4. **Armas de información:** recursos y métodos que se utilizan con el objeto de ocasionar daños a los recursos, procesos y sistemas de información de un Estado, ejercer influencia negativa en materia de información sobre los sistemas defensivos, administrativos, políticos, sociales, económicos y demás sistemas de importancia crítica de un Estado y también ejercer manipulación psicológica masiva de la población con el objeto de desestabilizar a una sociedad y un Estado.

5. **Seguridad de la información:** situación de protección de los intereses básicos de la persona, la sociedad y el Estado en la esfera de la información, inclusive la infraestructura de información y telecomunicaciones y la información propiamente tal en lo relativo a propiedades de ésta como integridad, objetividad, accesibilidad y confidencialidad.

6. **Amenazas a la seguridad de la información:** factores que comprometen los intereses básicos de la persona, la sociedad y el Estado en la esfera de la información.

7. **Seguridad internacional de la información:** situación de las relaciones internacionales tal que se impiden la violación de la estabilidad mundial y la creación de amenazas a la seguridad de los Estados y la comunidad internacional en la esfera de la información.

8. **Utilización ilegítima de los sistemas de información y telecomunicaciones y los recursos de información:** utilización de los sistemas y recursos de telecomunicaciones e información sin la autorización pertinente o en violación de las reglas establecidas, la legislación o las normas del derecho internacional.

9. **Injerencia no autorizada en los sistemas de información y telecomunicaciones y los recursos de información:** injerencia en los procesos de reunión, tratamiento, acumulación, almacenamiento, presentación, búsqueda, difusión y utilización de la información con el objeto de perturbar el funcionamiento normal de los sistemas de información o violar la integridad, confidencialidad y accesibilidad de los recursos de información.

10. **Estructuras de importancia crítica:** instalaciones, sistemas e instituciones de un Estado tales que la influencia premeditada sobre sus recursos de información puede tener consecuencias que afecten directamente la seguridad nacional (transporte, suministro de energía, la esfera crediticia y financiera, las comunicaciones, los órganos de la administración pública, el sistema de defensa, los órganos encargados de hacer cumplir la ley, los recursos de información estratégicos, las instalaciones científicas, las instalaciones de investigación y desarrollo, las instalaciones que pueden ocasionar peligro técnico y ecológico acrecentado y los órganos encargados de mitigar las consecuencias de los desastres naturales y otras situaciones de emergencia.

11. **Terrorismo internacional en la esfera de la información:** utilización de los sistemas y recursos de telecomunicaciones e información e influencia sobre dichos sistemas y recursos en la esfera de la información internacional con fines terroristas.

12. **Delincuencia internacional en materia de información:** utilización de los sistemas y recursos de telecomunicaciones e información e influencia sobre dichos sistemas y recursos en la esfera de la información internacional con fines ilegítimos.

**Principio I**

1. Las actividades de todo Estado y de otros sujetos del derecho internacional en la esfera de la información internacional deben contribuir al desarrollo social y económico común y realizarse de tal modo que sean compatibles con los objetivos del mantenimiento de la estabilidad y la seguridad mundiales, los derechos soberanos de los demás Estados, los intereses de la seguridad, los principios del arreglo pacífico de controversias y conflictos, la no utilización de la fuerza, la no injerencia en los asuntos internos y el respeto a los derechos y las libertades humanas.

2. Dichas actividades también deben ser compatibles con el derecho de cada persona a buscar, recibir y difundir información e ideas, tal como está establecido en los instrumentos pertinentes de las Naciones Unidas, habida cuenta de que dicho derecho puede ser limitado por la ley con el objeto de proteger los intereses de la seguridad de cada Estado.

3. Al mismo tiempo, cada Estado y los demás sujetos del derecho internacional deben tener iguales derechos a la protección de sus recursos de información y estructuras de importancia crítica de la utilización ilegítima y la injerencia no autorizada en materia de información y podrán contar con el apoyo de la comunidad internacional en el ejercicio de estos derechos.

**Principio II**

Los Estados se esforzarán en restringir las amenazas en la esfera de la seguridad internacional de la información y con este objeto se abstendrán de:

- a) La elaboración, creación y utilización de medios para ejercer influencia y ocasionar perjuicios en los recursos y sistemas de información de otro Estado;
- b) El ejercicio de influencia de información premeditada en estructuras de importancia crítica de otro Estado;
- c) El ejercicio de influencia en materia de información con el objeto de socavar los sistemas políticos, económicos y sociales de otros Estados y de manipular psicológicamente a una población con el objeto de desestabilizar a una sociedad;
- d) La injerencia no autorizada en los sistemas de información y telecomunicaciones y recursos de información, así como su utilización ilegítima;
- e) Acciones que conduzcan al dominio y el control en la esfera de la información;
- f) Impedimentos al acceso a las tecnologías más modernas de información y creación de condiciones de dependencia tecnológica en la esfera de la información en perjuicio de otros Estados;
- g) Estímulo a las actividades de asociaciones, organizaciones y grupos terroristas, extremistas y criminales internacionales, y de delincuentes particulares que constituyen una amenaza a los recursos de información y las estructuras de importancia crítica de los Estados;
- h) Elaboración y adopción de planes y doctrinas que prevean la posibilidad de librar una guerra de información y sean susceptibles de provocar una carrera de armamentos, así como de inducir tirantez en las relaciones entre los Estados y el estallido propiamente tal de guerras de información;

- i) Utilización de tecnologías y recursos de información en desmedro de los derechos y las libertades humanas básicas, ejercidos en la esfera de la información;
- j) Difusión transfronteriza de información en transgresión de los principios y las normas del derecho internacional, así como la legislación interna de determinados países;
- k) Manipulación de las corrientes de información, desinformación y ocultamiento de información con objeto de alterar el entorno psicológico y espiritual de una sociedad y erosionar los valores culturales, morales, éticos y estéticos tradicionales;
- l) Expansión en la esfera de información y adquisición de control sobre las infraestructuras nacionales de información y telecomunicaciones de otro Estado, incluidas las condiciones de su funcionamiento en la esfera de la información internacional.

### **Principio III**

Las Naciones Unidas y los organismos competentes del sistema de las Naciones Unidas fomentarán la cooperación internacional con objeto de restringir las amenazas en la esfera de la seguridad internacional de la información y crear con este objeto bases de derecho internacional para:

- a) Determinar los signos característicos de las guerras de información y clasificarlas;
- b) Determinar los signos característicos de las armas de información y su clasificación, así como los medios que pueden asimilarse a armas de información;
- c) Restringir el tráfico de armas de información;
- d) Prohibir la elaboración, difusión y utilización de armas de información;
- e) Impedir la amenaza del estallido de guerras de información;
- f) Reconocer el peligro de la utilización de armas de información contra estructuras de importancia crítica, que es comparable con el peligro de la utilización de armas de destrucción en masa;
- g) Crear condiciones para el intercambio de información internacional equitativo y seguro sobre la base de las normas y los principios generalmente reconocidos del derecho internacional;
- h) Impedir la utilización de las tecnologías y los recursos de información con fines terroristas y otros de índole criminal;
- i) Impedir la utilización de las tecnologías y los recursos de información para ejercer influencia sobre la conciencia colectiva con el objeto de desestabilizar a una sociedad y a un Estado;
- j) Elaborar procedimientos de notificación mutua y prevención del ejercicio de influencia transfronteriza no autorizada sobre la información;
- k) Crear sistemas de supervisión internacional para descubrir las amenazas que se manifiesten en la esfera de la información;
- l) Crear un mecanismo de verificación del cumplimiento de las condiciones del régimen de seguridad internacional de la información;

- m) Crear un mecanismo de solución de situaciones de conflicto en la esfera de la seguridad de la información;
- n) Crear un sistema internacional de certificación de las tecnologías y los recursos de la informática y las telecomunicaciones (inclusive los sistemas físicos y lógicos) como parte de las garantías de su seguridad internacional;
- o) Elaborar un sistema de cooperación internacional entre los órganos encargados de hacer cumplir la ley con el objeto de prevenir y reprimir las infracciones a la ley en la esfera de la información;
- p) Armonizar la legislación nacional a título voluntario con miras a garantizar la seguridad de la información.

#### **Principio IV**

Los Estados y otros sujetos del derecho internacional deberán asumir la responsabilidad internacional de las actividades en la esfera de la información que realicen bajo su jurisdicción o en el marco de organizaciones internacionales de las que sean miembros, así como de la conformidad de cualquier actividad de esa índole con los Principios que se establecen en el presente instrumento.

#### **Principio V**

Toda controversia entre Estados y otros sujetos del derecho internacional que surja de la aplicación de los presentes Principios se resolverá con ayuda de los procedimientos establecidos de arreglo pacífico de controversias.

### **Jordania**

[Original: árabe]  
[16 de mayo de 1999]

1. El uso de tecnología y sistemas de información tiene considerables ventajas para la comunidad internacional en relación con el mantenimiento de la estabilidad y la seguridad; no obstante, si se hace un mal uso de estos avances y nuevas tecnologías, ello tendrá como consecuencia:
  - a) Facilitar que redes terroristas se organicen mejor, al distribuirse sus miembros a lo largo de áreas geográficas muy amplias debido a las facilidades para establecer comunicaciones con rapidez;
  - b) Dificultar la vigilancia de las comunicaciones modernas, debido a la complejidad de las tecnologías, cada vez más rápidas y en constante evolución, y teniendo en cuenta la existencia, en la mayoría de los Estados, de leyes que, en defensa de la libertad de las personas, impiden interferir sus comunicaciones.
2. Movidos por nuestro interés por adoptar medidas correctas y en previsión de la comisión de cualquier acto terrorista, recomendamos lo siguiente:
  - a) Que se establezca o se revise una “ley especial de emergencia” que permita a las fuerzas de seguridad el acceso a los centros de control de las compañías que utilizan sistemas de comunicación avanzados, o su control parcial;

b) Que, en coordinación con las empresas o instituciones dedicadas a las telecomunicaciones, se capacite y cualifique a especialistas de las fuerzas del orden, a fin de que puedan manejar estos sistemas en caso de crisis;

c) Que se apoye al sector de la tecnología de sistemas de información y de telecomunicaciones y sus principios básicos en materia de seguridad, se cree una infraestructura y se preste la capacitación adecuada, para ayudar al mantenimiento de la paz y la seguridad internacionales.

## **Qatar**

[Original: árabe]  
[17 de mayo de 1999]

1. **Espionaje:** Debe impedirse que una parte no autorizada tenga acceso al contenido de los sistemas de información y de telecomunicaciones internacionales.

2. **Sabotaje:** Debe impedirse el sabotaje parcial o total de los sistemas de información y de telecomunicaciones internacionales.

3. **Registro de datos:** Deben registrarse los datos enviados por medio de sistemas de información y de telecomunicaciones, incluyendo la propiedad intelectual.

4. **Falsificación:** Debe lucharse contra la falsificación de datos enviados por medio de sistemas de información y de telecomunicaciones internacionales.

5. **Protección:** Debe desarrollarse la protección electrónica de datos enviados por medio de sistemas de información y de telecomunicaciones internacionales.

6. **Legislación:** Deben aprobarse las leyes necesarias para regular todas las transacciones electrónicas y garantizar los derechos de quienes las efectúan, castigando a sus infractores.