Naciones Unidas A/56/164/Add.1

Asamblea General

Distr. general
3 de octubre de 2001
Español
Original: ruso

Quincuagésimo sexto período de sesiones
Tema 69 del programa
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

01-56160 (S) 111001 111001

II. Respuestas recibidas de los Gobiernos

Federación de Rusia

[Original: ruso]
[21 de junio de 2001]

Evaluación general de los problemas de la seguridad de la información

Peligros para la seguridad internacional de la información

En el párrafo 1 de su resolución 55/28, la Asamblea General insta a los Estados Miembros a que sigan promoviendo el examen de los peligros actuales y posibles en el ámbito de la seguridad de la información. En el proyecto de documento presentado por la Federación de Rusia titulado "Principios relativos a la seguridad internacional de la información" (véase A/55/140, secc. II), los peligros para la seguridad de la información consisten en factores que ponen en riesgo los intereses básicos de la persona, la sociedad y el Estado en el ámbito de la información.

Según opina la Federación de Rusia, entre esos factores básicos se cuentan los siguientes:

1. **Elaboración, creación y utilización de medios para ejercer influencia sobre los recursos de información y los sistemas de telecomunicaciones de otro Estado o para dañarlos**

- Medios de influencia radioelectrónica o de interferencia electromagnética utilizados por formaciones armadas ilegales (anticonstitucionales), grupos terroristas y particulares con objeto de inutilizar temporal o irreversiblemente los medios y sistemas radioelectrónicos;
- Medios de influir en los recursos programáticos de módulos electrónicos de control con el fin de inutilizarlos o de modificar el algoritmo de su funcionamiento;
- Medios de influir en el proceso de transmisión de información con objeto de interrumpirlo o desorganizarlo mediante la modificación del medio de transmisión de las señales y los algoritmos de funcionamiento;
- Medios de desinformación dirigidos a crear en el ámbito de la información un cuadro virtual de la situación que difiere de la realidad o que la tergiversa directamente;
- Medios de influir en la psiquis y el subconsciente de la persona con el fin de desorientarla, quebrantar su voluntad o incapacitarla temporalmente.

2. **Utilización deliberada de la información para ejercer influencia en las estructuras vitales de otro Estado**

Resulta particularmente peligrosa la utilización del arma de la información contra objetivos militares y civiles y los sistemas e instituciones de un Estado, el trastorno de cuyo funcionamiento normal pone en peligro directamente la seguridad nacional.

Por ejemplo, la penetración no autorizada en los sistemas de control computadorizados de las centrales eléctricas puede provocar la paralización total de la infraestructura de los servicios vitales de un país, y si llegara a tratarse de centrales electronucleares podría tener consecuencias catastróficas, semejantes a la tragedia de Chernobyl.

El acceso no autorizado de asociaciones delictivas y terroristas a la información sobre proyectos científico-técnicos relacionados con la defensa o de doble uso podría permitirles producir tipos novedosos de armas para ser utilizadas con fines delictivos y también para fines de chantaje político.

Las bases de datos y demás recursos de información de los órganos judiciales podrían distorsionarse o quedar totalmente destruidos mediante una interferencia informativa desde fuera, con lo cual se obstaculizaría gravemente la administración de la justicia, la lucha eficaz contra la delincuencia y el mantenimiento de la legalidad y el orden público.

La influencia ejercida sobre los recursos de información en el ámbito financiero-crediticio como la transferencia no autorizada o el desfalco directo de recursos bancarios, la reducción de cuentas a saldo cero o, peor aún, el bloqueo de las redes computadorizadas centrales de las instituciones bancarias mediante "ataques electrónicos", podría provocar evidentemente situaciones de crisis no sólo en esa esfera concreta sino incluso el colapso general de la economía de un país, y, en consecuencia, a complicar gravemente sus relaciones internacionales.

Una arremetida en masa contra la infraestructura de las telecomunicaciones mediante la utilización del arma de la información provocaría el bloqueo de los sistemas de dirección y de adopción de decisiones de un Estado.

La utilización de la información como medio de ejercer una influencia hostil en los sistemas de comunicación y control de los sistemas de defensa antiaérea, de defensa contra misiles y de otros sistemas de defensa deja desarmado a un Estado ante un posible agresor impidiéndole ejercer el derecho de legítima defensa.

La desorganización provocada del proceso de producción en las empresas de tecnología avanzada o que entrañan posibles riesgos para el medio ambiente (la producción de sustancias químicas, biológicas y de combustibles) podría provocar consecuencias no menos desastrosas.

La desorganización de los medios de comunicación, control y transporte de los servicios relacionados con el salvamento de seres humanos y la eliminación de las consecuencias de desastres naturales o de otras situaciones de emergencia podría aumentar considerablemente los daños materiales y la pérdida de vidas humanas en situaciones de ese tipo.

3. Utilización de la información con el objeto de socavar el sistema político y social de un Estado, así como la manipulación sicológica de una población con el objetivo de desestabilizar la sociedad

La utilización intencional de la información como medio de ejercer influencia sobre el enemigo (un adversario u opositor) no es una idea novedosa. No obstante, hoy día, gracias a la amplísima difusión de modernas tecnologías de las telecomunicaciones y la creación de redes mundiales de información, esos medios de ejercer influencia ofrecen posibilidades cualitativamente distintas. La posibilidad de llevar a cabo acciones de carácter masivo y total en la esfera de la información ha contribuido a que el arma de la información haya dejado de considerarse un medio auxiliar para pasar a ser un instrumento de enfrentamiento fundamental.

Al propio tiempo, la esfera de la información adquiere un carácter de factor fundamental de creación de sistemas en la vida de cualquier sociedad e influye activamente en prácticamente todas las dimensiones de la seguridad de un Estado. Esa dependencia aumentará en la medida en que se realicen progresos en la esfera de la tecnología de la información. La información como elemento de presión predominante derivada de la preponderancia de un círculo limitado de fuentes de información podría utilizarse para ejercer una influencia deliberada y negativa en la psiquis de la población de un país en su conjunto, o en el personal de instituciones vitales, el aparato administrativo y gubernamental y los órganos legislativos de un país.

La inculcación de la incapacidad de resolver problemas personales, la desconfianza en las instituciones oficiales y la desesperanza; el quebrantamiento de la voluntad; y la provocación de contradicciones por motivos religiosos, étnicos o sociales contribuyen a socavar los cimientos del Estado y a desestabilizar la sociedad. En resumen, ese tipo de situaciones puede dar lugar a la estratificación antagónica de grupos sociales, desembocar en una guerra civil y terminar en la desintegración total del Estado.

4. Injerencia no autorizada en los sistemas de información y telecomunicaciones y en los recursos de información, y uso ilícito de estos sistemas y recursos

Hoy día prácticamente todos los Estados hacen frente o pueden verse en la necesidad de hacer frente a actos de injerencia no autorizada en sus sistemas de información, fenómeno que evidentemente tiende a aumentar. El peligro de esa injerencia estriba en que puede dar lugar a una sucesión de consecuencias peligrosas: la experiencia de los piratas informáticos la aprovechan las agrupaciones delictivas, mientras que sus “logros” podrían utilizarse como un arma para llevar a cabo acciones hostiles, incluso militares, entre los Estados.

El actual nivel de desarrollo socioeconómico contribuye a su vez a agudizar las contradicciones entre la necesidad que tiene la sociedad de ampliar el intercambio y acceso libres a la información, por una parte, y, por otra, la necesidad evidente de establecer restricciones reglamentarias a ese intercambio y acceso.

Al propio tiempo, la injerencia no autorizada en los sistemas de información o su uso ilícito, en los casos en que se reconoce como tal en las leyes y normas nacionales, se interpreta de maneras muy diversas, que abarcan desde una mera infracción administrativa hasta un delito penado por la ley. En general, muchos países no han adoptado una postura definida a ese respecto.

En consecuencia, valiéndose de las ramificaciones de las redes de información internacionales desde su propio territorio y sin violar las leyes de su país, el infractor puede quedar fuera del alcance de la jurisdicción del Estado cuyas leyes, de hecho, ha transgredido.

Una solución podría ser que se perfeccionara la tecnología destinada a brindar protección a las redes de información, si bien eso sólo lo podrían emprender los Estados que reunieran las condiciones técnicas, y, sobre todo financieras, necesarias.

Es evidente que esa situación conducirá lógicamente a la necesidad de que se codifique la legislación nacional vigente y se cree una base de derecho internacional universal encargada de prever dichas infracciones y delitos.

5. Adopción de medidas para dominar y controlar el ámbito de la información

En lo que respecta al ámbito de la información, el proceso de mundialización se caracteriza, además, por poseer un nivel más elevado de normalización, lo que facilita que los países desarrollados desde el punto de vista económico y de la información penetren los mercados de las telecomunicaciones de los países en desarrollo. Los países menos adelantados no tienen otra opción que no sea adoptar esas normas y permitir que se utilicen las nuevas tecnologías en su ámbito de información. En el marco de un mercado liberalizado de la tecnología de la información y el libre intercambio de la información, los países desarrollados ocupan una posición dominante respecto de otros Estados, factor que puede utilizarse en detrimento de sus intereses en materia de seguridad nacional.

6. Obstaculización del acceso a las tecnologías de la información más novedosas y creación de relaciones de dependencia tecnológica en la esfera de la información en detrimento de otros Estados

Las causas por las que puede obstaculizarse o restringirse la obtención por otros países de las tecnologías de la información más novedosas son, al parecer, análogas a las que surgen en relación con otras tecnologías avanzadas. Por una parte, esas restricciones pueden obedecer a consideraciones puramente económicas o a un deseo de monopolizar un sector del mercado y, por otra, pueden deberse a razones políticas (por ejemplo, la imposición de sanciones, la adopción de medidas de respuesta respecto de países “poco amistosos”, así como consideraciones relacionadas con la seguridad del país). En uno y otro caso no puede descartarse la intención de mantener o crear en la esfera de la información una relación de dependencia tecnológica de unos países respecto de otros.

En todo caso, el carácter decisivo que para cualquier país adquieren en el siglo XXI las tecnologías de la información obliga a plantear el acceso a ellas como un problema vital.

También debe tenerse en cuenta una característica propia de la creación del arma de la información que consiste en que las tecnologías de la información que se emplean con ese fin inicialmente surgen, por regla general, en el sector civil y sólo después suelen transferirse al sector militar.

Habida cuenta de esos factores, es evidente que la cuestión de la restricción del acceso a las tecnologías de la información debe plantearse exclusivamente en relación con la prevención de su utilización como arma, la creación por medio de ellas de nuevos tipos destructivos de armas o la utilización de esas tecnologías con fines ilícitos o para propósitos que no responden a los objetivos generales de la seguridad. Cualesquiera otros motivos que puedan esgrimirse para restringir el marco del futuro régimen de seguridad internacional de la información se considerarán inaceptables.

7. Adopción de medidas por asociaciones, organizaciones o grupos internacionales de terroristas, extremistas o delincuentes o por delincuentes aislados que pongan en peligro las estructuras vitales y los recursos de información de un Estado

El desarrollo sin precedentes de los sistemas institucionales, estatales e internacionales de la información y la ampliación simultánea de las posibilidades de acceso a esos sistemas han alcanzado un nivel tal que prácticamente todos los miembros de la comunidad internacional encaran hoy día el peligro real de ser blanco de una agresión electrónica por parte de delincuentes y terroristas. Característicamente, la magnitud de ese peligro crecerá en la medida en que se desarrolle la infraestructura mundial de esos sistemas y, por consiguiente, adquirirá un carácter transfronterizo.

Tanto la delincuencia de la información como el terrorismo de la información representan actividades ilícitas que, no obstante, difieren entre sí por el carácter

de los propósitos que se plantea cada cual. Si el delincuente de la información responde a necesidades estrictamente egoístas o propias del malhechor, los terroristas utilizan el ciberespacio para fines propios del terrorismo político en general.

Entre los medios que se utilizan para llevar a cabo esas actividades pueden contarse diversos tipos de armas de la información.

Valiéndose de programas, la técnica y las tecnologías especiales de la informática, los terroristas son capaces de lograr lo siguiente:

- Destruir, tergiversar y manipular diversos elementos de la infraestructura de la información;
- Sustraer información importante;
- Modificar información oficial y fáctica con fines propios;
- Ocupar y bloquear canales de los medios de difusión para difundir desinformación, propagar rumores dirigidos a crear pánico, difundir amenazas de actos de terrorismo y divulgar sus demandas;
- Inutilizar los sistemas de comunicación creando una sobrecarga artificial;
- Difundir amenazas de actos de terrorismo en el ámbito de la información que entrañen graves consecuencias políticas, económicas, sociales u otras consecuencias peligrosas.

La táctica del terrorismo de la información consiste en lograr que el acto de terrorismo entrañe consecuencias peligrosas, que llegue a ser de conocimiento generalizado y que tenga una amplia resonancia social. Lamentablemente, los sistemas de información carentes de protección ofrecen amplísimas posibilidades para llevar a cabo esas actividades.

8. Formulación y adopción por los Estados de planes o doctrinas que incluyan la posibilidad de hacer la guerra en el campo de la información y puedan provocar una carrera de armamentos y generar tensiones en las relaciones entre los Estados y conducir a guerras de información per se

Una de las principales orientaciones de la actual estrategia de defensa de muchos Estados tecnológicamente desarrollados consiste en adquirir un poderío en materia de información que presupone un potencial de información militar de carácter tanto defensivo como ofensivo. Esa estrategia se plasma en las respectivas doctrinas nacionales. En vista de que ha aumentado el papel de la guerra de la información y de los medios de enfrentamiento en la esfera de la información se someten a revisión los conceptos tradicionales de la amenaza a la soberanía nacional y a la observancia de los principios y normas del derecho internacional; de la naturaleza de la competencia económica; y del papel de los Estados en los asuntos internacionales. A ese respecto, se asigna cada vez mayor atención a la guerra estratégica de la información como nueva categoría de conflicto.

La conjugación del poderío económico y el poderío en materia de información permite ejercer una influencia efectiva en la evolución de la política internacional sin tener que recurrir a los medios tradicionales y "burdos" de coerción basados en la utilización de la fuerza armada.

Esas nuevas estrategias se fundamentan en las siguientes características:

- El desarrollo de tecnologías de la información no suscita en la opinión pública la misma reacción en extremo negativa que el aumento de las armas corrientes, sobre todo si se trata de armas de destrucción en masa;
- El apoyo al desarrollo de sistemas de información es útil por cuanto esos sistemas son más compatibles con el concepto de tecnologías de doble uso y en muchos casos pueden utilizarse simultáneamente para fines tanto militares como civiles y comerciales;
- Al marchar a la vanguardia del desarrollo y la aplicación de las tecnologías de la información el Estado consolida su monopolio sobre el dominio de la información estratégica y, en consecuencia, sobre la posibilidad de reaccionar de manera más operacional en caso de que aumente la tensión internacional.

Al propio tiempo, se considera que la aplicación del arma de la información puede contribuir a disminuir considerablemente las bajas y pérdidas en comparación con las acciones armadas "tradicionales". Es evidente que, con ello se pretende crear la impresión de que las operaciones en la esfera de la información revisten un "carácter humanitario".

Sin embargo, todos los Estados son conscientes de las ventajas y los peligros que entraña el desarrollo de las tecnologías de la información, por lo que procurarán reaccionar debidamente a la evolución de la situación. La elaboración ulterior de planes y doctrinas de la guerra de la información tenderá a propiciar un aumento considerable del número de países que disponen de un arsenal de la información y, por consiguiente, desencadenar una carrera de armamentos en un nuevo plano tecnológico. En suma, la situación imperante actualmente en la esfera del control de los armamentos podría revertir a las condiciones características del período de la guerra fría.

9. Utilización de los medios y tecnologías de la información en detrimento de las libertades y los derechos humanos en la esfera de la información

Los intereses de la persona en materia de información consisten en que se le garantice el ejercicio de sus derechos y libertades respecto del acceso a la información; la utilización de la información en actividades lícitas y el desarrollo espiritual e intelectual; la confidencialidad en el plano personal y familiar; la inviolabilidad de la correspondencia y demás intercambios por medio de las telecomunicaciones; y la protección del honor y la dignidad de la persona.

Hoy día, el desarrollo y la amplia aplicación de las tecnologías y los medios de la información nuevos ofrecen posibilidades sin precedentes para el ejercicio del derecho a la información. No obstante, los avances registrados en la informatización de la vida social y el desarrollo de redes de información contribuyen a que se amplíe el acceso a un volumen cada vez mayor de datos relativos a la vida personal de los ciudadanos por conducto de las bases de datos de dominio público. Por otra parte, surge el peligro de que las autoridades restrinjan ilícitamente el acceso de la población a los recursos de información de dominio público de los órganos federales, los órganos de gobierno local, los archivos y otras fuentes de información de dominio público de valor social.

En el futuro régimen de seguridad internacional de la información deberá preverse la prohibición unificada de reunir, conservar, utilizar y difundir información sobre la vida de particulares sin su consentimiento y de restringir el acceso de la población a la información, salvo en los casos previstos en la ley.

10. Difusión transfronteriza no controlada de la información en contravención de los principios y normas del derecho internacional y de las leyes nacionales de países concretos

La mundialización del ámbito de la información trastorna los conceptos tradicionales de fronteras geográficas, estatales y administrativas o zonas de competencia en lo que respecta a la tarea de garantizar la seguridad nacional. En ese marco surge la necesidad de definir con precisión las fuentes de los peligros, ya sean éstas de carácter interno o externo. Por ejemplo, una operación militar hostil basada en la utilización de información contra otro Estado puede enmascararse como una acción de delincuentes “locales”. Es decir, los Estados que anteriormente eran capaces de garantizar el régimen jurídico del intercambio de la información dentro de sus fronteras resultan indefensos en las nuevas circunstancias ante la penetración de su territorio desde fuera de información de difusión prohibida o de carácter destructivo (la pornografía; la desinformación; la información dirigida a promover la discriminación e intolerancia raciales; la información destinada a instigar la hostilidad social, nacional o religiosa; y la información de carácter subversivo difundida y utilizada por grupos de delincuentes y terroristas internacionales).

11. Manipulación de las corrientes de información, la desinformación y el ocultamiento de información con el fin de debilitar el entorno espiritual y psicológico de una sociedad y socavar sus valores culturales, morales, éticos y estéticos tradicionales

El carácter de los medios de información y/o de la información como elemento de influencia puede modificar sustancialmente la conciencia de las masas y la conducta de importantes grupos sociales. Reviste un peligro especial, al respecto, la forma de ejercer influencia conocida como manipulación, un tipo de influencia psicológica encaminada a estimular en la persona o un grupo social propósitos que no coinciden con la realidad. Una situación política inestable o de tirantez contribuye a intensificar la “eficacia” de la manipulación de la información. La difusión en masa de desinformación o, por el contrario, el ocultamiento de información veraz en situaciones como éstas, tiene por objeto impedir que los hechos y factores puedan valorarse objetivamente. La opinión pública es sumamente susceptible a ese tipo de influencia.

Reforzadas con todo el poderío de la estructura moderna de la información, esas operaciones pueden contribuir a destruir el entorno psicológico y los valores culturales y espirituales de la sociedad (la guerra de las culturas). A su vez, la desmoralización crea las premisas necesarias para la disolución de la autoconciencia nacional y el quebrantamiento de la voluntad de oponer resistencia a una posible agresión.