Naciones Unidas A/65/201

Asamblea General

Distr. general
30 de julio de 2010
Español
Original: inglés

Sexagésimo quinto período de sesiones
Tema 94 del programa provisional*
Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional

Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional

Nota del Secretario General

El Secretario General tiene el honor de remitir adjunto el informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. El Grupo fue creado en cumplimiento de lo dispuesto en el párrafo 4 de la resolución 60/45 de la Asamblea General.

* A/65/150.

10-46960 (S) 180810 180810

Informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional

Resumen

Las amenazas reales y potenciales en la esfera de la seguridad de la información constituyen algunos de los problemas más graves del siglo XXI. Las amenazas derivan de una amplia gama de fuentes y se manifiestan como actividades desestabilizadoras dirigidas por igual contra particulares, empresas, elementos de la infraestructura nacional y gobiernos. Sus efectos entrañan considerables riesgos para la seguridad pública, la seguridad de las naciones y la estabilidad de la comunidad internacional en su conjunto.

El uso creciente de las tecnologías de la información y las comunicaciones en infraestructuras esenciales crea nuevos puntos vulnerables y oportunidades para la desestabilización. Debido a la compleja interconectividad de las telecomunicaciones y de Internet, cualquier dispositivo de las tecnologías de la información y las comunicaciones puede llegar a ser una fuente o blanco de un uso indebido cada vez más refinado. Puesto que estas tecnologías son, por su naturaleza, de doble uso, las mismas tecnologías que apoyan a un robusto comercio electrónico pueden utilizarse también para amenazar la paz internacional y la seguridad nacional.

El origen de la desestabilización, la identidad del autor o los móviles pueden resultar difíciles de determinar. Frecuentemente los autores de estas actividades pueden deducirse por los blancos elegidos, los efectos provocados u otras pruebas evidenciarias, y pueden estar situados prácticamente en cualquier lugar del mundo. Estas características facilitan el empleo de las tecnologías de la información y las comunicaciones para causar perturbaciones. La incertidumbre en cuanto a la atribución y la falta de una comprensión común crea el riesgo de inestabilidad y de percepciones erróneas.

Cada vez son más numerosos los informes de que los Estados están desarrollando tecnologías de la información y las comunicaciones como instrumentos de guerra y para fines de inteligencia y políticos. Cada vez son motivo de mayor preocupación los particulares, los grupos u organizaciones, incluidas las organizaciones delictivas, que emprenden por cuenta de terceros actividades desestabilizadoras en línea. El refinamiento y la escala crecientes de la actividad delictiva aumentan la probabilidad de actos perjudiciales. Si bien es cierto que no son muchas las indicaciones de uso terrorista de las tecnologías de la información y las comunicaciones para ejecutar operaciones desestabilizadoras, es posible que dicho uso se intensifique en el futuro.

La lucha contra estos problemas del siglo XXI depende del éxito de la cooperación entre asociados movidos por ideas similares. La colaboración entre los Estados y entre los Estados y el sector privado y la sociedad civil, es importante y las medidas para mejorar la seguridad de la información exigen una amplia cooperación internacional si han de resultar eficaces. El informe del Grupo de Expertos Gubernamentales ofrece recomendaciones para proseguir el diálogo entre los Estados a fin de reducir los riesgos y proteger la infraestructura nacional e internacional esencial.

Índice

Prólogo del Secretario General

Hace una década no hubiéramos podido prever hasta qué punto las tecnologías de la información y las telecomunicaciones quedarían integradas en nuestras vidas cotidianas o en qué medida llegaríamos a depender de ellas. Estas tecnologías han creado una comunidad internacional interconectada y, si bien esta interconexión global reporta inmensos beneficios, también crea puntos vulnerables y riesgos.

Se han hecho considerables progresos en la forma de encarar las consecuencias de las nuevas tecnologías. Pero la tarea es ardua y apenas hemos empezado a elaborar las normas, leyes y modalidades de cooperación necesarias para manejarnos en este nuevo entorno de la información.

Teniendo eso presente, designé a un Grupo de Expertos Gubernamentales de 15 Estados para que estudiaran las amenazas reales y potenciales en esta esfera y recomendasen los medios de abordarlas. Doy las gracias a la Presidencia del Grupo y a los Expertos por su concienzuda y diligente labor, que ha producido el presente informe, exposición concisa del problema y los posibles pasos a seguir.

La Asamblea General tiene un importante papel que desempeñar en el proceso de lograr que las tecnologías de la información y las telecomunicaciones sean más seguras, tanto en el plano nacional como en el internacional. Será esencial que los Estados Miembros entablen el diálogo para elaborar perspectivas comunes. También es vital la cooperación con espíritu pragmático, compartir las mejores prácticas, intercambiar información y crear capacidad en los países en desarrollo además de reducir el riesgo de percepciones erróneas, que podrían entorpecer la capacidad de la comunidad internacional para hacer frente a los incidentes graves en el ciberespacio.

Tenemos un nutrido programa para nuestra futura labor. El presente informe tiene por objeto servir a manera de paso inicial hacia el establecimiento del marco internacional para la seguridad y la estabilidad que exigen estas nuevas tecnologías. Recomiendo que los Estados Miembros y el público mundial en general presten atención al análisis y las recomendaciones que en él se hacen.

Carta de envío

16 de julio de 2010

Tengo el honor de presentar el informe del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional. El Grupo fue creado en 2009 en cumplimiento de lo dispuesto en el párrafo 4 de la resolución 60/45 de la Asamblea General. Como Presidente del Grupo me complace declarar que el informe se aprobó por consenso.

En esa resolución, titulada "Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional", la Asamblea General pidió que se estableciera en 2009 un grupo de expertos gubernamentales sobre la base de una distribución geográfica equitativa, para que continuara examinando las amenazas reales y potenciales en el ámbito de la seguridad de la información y las posibles medidas de cooperación para encararlas, así como los conceptos encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones. Se pidió al Secretario General que presentara un informe sobre los resultados de ese estudio a la Asamblea General en su sexagésimo quinto período de sesiones.

De conformidad con lo dispuesto en la resolución, se designó a expertos de 15 Estados: Alemania, Belarús, Brasil, China, Estados Unidos de América Estonia, Federación de Rusia, Francia, India, Israel, Italia, Qatar, Reino Unido de Gran Bretaña e Irlanda del Norte, República de Corea y Sudáfrica. La lista de expertos figura en el anexo.

El Grupo de Expertos Gubernamentales celebró cuatro períodos de sesiones: el primero del 24 al 26 de noviembre de 2009, en Ginebra; el segundo, del 11 al 15 de enero de 2010, en la Sede de las Naciones Unidas; el tercero, del 21 al 25 de junio de 2010, en Ginebra; y el cuarto, del 12 al 16 de julio, en la Sede de las Naciones Unidas.

En las reuniones del Grupo hubo un intercambio amplio y profundo de opiniones sobre las novedades en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional. Además, el Grupo tuvo en cuenta las opiniones expresadas en las respuestas enviadas por los Estados Miembros en cumplimiento de lo pedido en las resoluciones 60/45, 61/54, 62/17 y 63/37 de la Asamblea General tituladas "Los avances a la información y las telecomunicaciones en el contexto de la seguridad internacional", así como las contribuciones y monografías de antecedentes aportadas por distintos miembros del Grupo.

El Grupo desea expresar su reconocimiento por la contribución aportada por el Instituto de las Naciones Unidas de Investigación sobre el Desarme, que prestó asesoramiento al Grupo y estuvo representado por James Lewis y Kerstin Vignard. El Grupo también desea dar las gracias a Ewen Buchanan, Oficial de Información de la Subdivisión de Información y Actividades de Extensión de la Oficina de Asuntos de Desarme de la Secretaría, que se desempeñó como secretario del Grupo, y a otros funcionarios de la Secretaría que prestaron su asistencia al Grupo.

(*Firmado*) Andrey V. **Krustskikh**
Presidente del Grupo

I. Carta de envío

1. Las amenazas reales y potenciales en la esfera de la seguridad de la información se cuentan entre los problemas más graves del siglo XXI. Estas amenazas pueden ocasionar daños considerables en las economías y en la seguridad nacional e internacional. Las amenazas proceden de una amplia gama de fuentes y se manifiestan en actividades desestabilizadoras dirigidas contra particulares, empresas, elementos de la infraestructura nacional y gobiernos. Sus efectos entrañan considerables riesgos para la seguridad pública, la seguridad de las naciones y la estabilidad de una comunidad internacional intercontectada.

2. Las tecnologías de la información y las comunicaciones tienen características únicas en su género que hacen difícil la tarea de encarar las amenazas que enfrentan los Estados y otros usuarios. Las tecnologías de la información y las comunicaciones están en todas partes y son de fácil acceso. No son de naturaleza intrínsicamente civil ni militar y el destino que se les dé depende principalmente de los móviles del usuario. En muchos casos las redes son propiedad y están bajo la dirección del sector privado o de particulares. Debido a la compleja interconectividad de las telecomunicaciones y de Internet, cualquier dispositivo de tecnologías de la información y las comunicaciones puede ser fuente o blanco de un uso indebido cada vez más refinado. Es muy fácil encubrir el uso malicioso de estas tecnologías. Puede resultar difícil establecer el origen de una perturbación, la identidad del autor o sus móviles. Con frecuencia, los autores de dichas actividades pueden deducirse solo por la elección de los blancos, los efectos producidos o las pruebas indiciarias. Los creadores de amenazas pueden operar fundamentalmente con impunidad, prácticamente desde cualquier punto del mundo. Estas características facilitan el empleo de estas tecnologías en actividades desestabilizadoras.

3. Teniendo en cuenta las consecuencias de esta evolución para la seguridad internacional, la Asamblea General de las Naciones Unidas pidió al Secretario General que, con la asistencia de expertos gubernamentales, estudiara las amenazas en el ámbito de la seguridad de la información y los conceptos internacionales pertinentes y sugiriese posibles medidas de cooperación para fortalecer la seguridad de los sistemas mundiales de información y de comunicaciones.

II. Amenazas, riesgos y puntos vulnerables

4. La red mundial de tecnologías de la información y las comunicaciones se ha convertido en teatro de actividades desestabilizadoras. Los motivos para crear inestabilidad varían profundamente y van desde el deseo de demostrar simplemente habilidad técnica, al robo de dinero o de información, pasando por su empleo en conflictos estatales. Las fuentes de esas amenazas incluyen agentes no estatales, como delincuentes y, quizás, hasta terroristas, así como los propios Estados. Estas tecnologías pueden ser utilizadas para dañar los recursos e infraestructuras de información. Dado que por su naturaleza intrínseca son de doble uso, las mismas tecnologías que prestan apoyo a un robusto comercio electrónico pueden utilizarse también para comprometer la paz internacional y la seguridad nacional.

5. Muchas herramientas y metodologías de uso malicioso tienen su origen en las actividades de delincuentes y piratas informáticos. El refinamiento y la escala crecientes de la actividad delictiva aumenta la probabilidad de actos perjudiciales.

6. Hasta ahora, ha habido pocos indicios de tentativas terroristas de comprometer o incapacitar la infraestructura de las tecnologías de la información y las comunicaciones o de ejecutar operaciones utilizando estas tecnologías, si bien puede suceder que se intensifiquen en el futuro. Actualmente los terroristas recurren a estas tecnologías principalmente para comunicarse, reunir información, reclutar miembros, organizarse, promover sus ideas y actividades y solicitar fondos, pero en algún momento podrían llegar a usarlas para sus ataques.

7. Cada vez son más frecuentes los informes de que los Estados están elaborando tecnologías de la información y las comunicaciones como instrumentos de guerra y para fines de inteligencia y políticos. La incertidumbre en cuanto a la atribución y la ausencia de una comprensión común respecto de lo que es una conducta estatal aceptable pueden crear el riesgo de inestabilidad y percepciones erróneas.

8. Motivo de creciente preocupación son las personas, grupos u organizaciones, incluidas las organizaciones delictivas, que se dedican por cuenta de terceros a realizar actividades desestabilizadoras en línea. Estos agentes, sea que estén motivados por ánimo de lucro o por otras razones, pueden ofrecer toda una gama de servicios maliciosos a agentes estatales y no estatales.

9. El uso cada vez más difundido de las tecnologías de la información y las comunicaciones en infraestructuras esenciales crea nuevos puntos vulnerables y oportunidades para crear inestabilidad, al igual que el empleo creciente de dispositivos de comunicaciones móviles y servicios con base en Internet.

10. Los Estados también se sienten inquietos debido a que la cadena de suministro de estas tecnologías puede resultar influida o subvertida de maneras que afectarían el uso normal, seguro y fiable de esas tecnologías. La inclusión de funciones ocultas maliciosas en las tecnologías puede socavar la confianza en los productos y servicios, erosionar la fe en el comercio y afectar la seguridad nacional.

11. El hecho de que existan distintos grados de capacidad y seguridad en cuanto a las tecnologías de la información y las comunicaciones entre los diferentes Estados aumentan la vulnerabilidad de la Red Mundial. Las diferencias en las leyes y prácticas nacionales pueden crear obstáculos a la creación de un entorno digital seguro y resistente.

III. Medidas de cooperación

12. Los riesgos que entrañan las redes con interconexiones mundiales exigen respuestas concertadas. En la última década, los Estados Miembros han afirmado reiteradamente la necesidad de recurrir a la cooperación internacional para combatir las amenazas en el ámbito de la seguridad de las tecnologías de la información y las comunicaciones y luchar contra el uso indebido y delictivo de la tecnología de la información, crear una cultura global de ciberseguridad y promover otras medidas esenciales capaces de reducir el riesgo.

13. Durante la última década se han hecho esfuerzos por combatir la amenaza de la ciberdelincuencia en el plano internacional, en particular, en el seno de la

Organización de Cooperación de Shangai, la Organización de los Estados Americanos, el Foro de Cooperación Económica de Asia y el Pacífico, el Foro Regional de la Asociación de Naciones de Asia Sudoriental (ASEAN), la Comunidad Económica de los Estados de África Occidental, la Unión Africana, la Unión Europea, la Organización para la Seguridad y la Cooperación en Europa y el Consejo de Europa, así como en el contexto de iniciativas bilaterales entre Estados.

14. También debería prestarse suficiente atención a esferas no delictivas de preocupación transnacional. Cabe mencionar, entre ellas, el riesgo de percepciones erróneas resultantes de la falta de conocimientos compartidos en cuanto a las normas internacionales que rigen el uso por los Estados de las tecnologías de la información y las comunicaciones, lo cual podría afectar la gestión de las crisis en caso de incidentes graves. Esto constituye un buen argumento para la elaboración de medidas concebidas para estrechar la cooperación en lo posible. Dichas medidas podrían diseñarse también para compartir las mejores prácticas, gestionar los incidentes, fomentar la confianza, reducir los riesgos y aumentar la transparencia y la estabilidad.

15. A medida que las actividades desestabilizadoras que utilizan tecnologías de la información y las comunicaciones se vayan haciendo más complejas y peligrosas, es evidente que ningún Estado podrá hacer frente solo a estas amenazas. No se podrá hacer frente a los retos del siglo XXI sin una cooperación productiva entre asociados con convicciones similares. La colaboración entre los Estados, y entre los Estados con el sector privado y la sociedad civil, es importante y las medidas encaminadas a mejorar la seguridad de la información exigen una amplia cooperación internacional si han de resultar eficaces. Por consiguiente, la comunidad internacional debería considerar la necesidad de establecer iniciativas y mecanismos cooperativos.

16. En los acuerdos existentes figuran normas pertinentes para el uso de las tecnologías de la información y las comunicaciones por los Estados. Dadas las características de las tecnologías de la información y las comunicaciones, únicas en su género, podrían elaborarse normas adicionales con el transcurso del tiempo.

17. La creación de capacidad es de vital importancia para lograr el éxito en la tarea de garantizar la seguridad mundial de las tecnologías de la información y las comunicaciones, asistir a los países en desarrollo en sus esfuerzos por acrecentar la seguridad de su infraestructura nacional de información, de importancia crítica, y remediar la disparidad actual en la seguridad de las tecnologías de la información y las comunicaciones. Hará falta una estrecha cooperación internacional para crear capacidad en los Estados que puedan necesitar asistencia para abordar el problema de la seguridad de sus tecnologías de la información y las comunicaciones.

IV. Recomendaciones

18. Teniendo en cuenta las amenazas reales y potenciales, los riesgos y puntos vulnerables en la esfera de la seguridad de la información, el Grupo de Expertos Gubernamentales considera de utilidad recomendar que se adopten nuevas medidas para el fomento de la confianza y para reducir el riesgo de las percepciones erróneas resultantes de las perturbaciones de las tecnologías de la información y las comunicaciones por ejemplo:

i) Proseguir el diálogo entablado entre los Estados para examinar las normas relativas al uso de las tecnologías de la información y las comunicaciones por los Estados, reducir los riesgos colectivos y proteger los elementos esenciales de la infraestructura nacional e internacional;

ii) Adoptar medidas de fomento de la confianza, de estabilidad y de reducción de los riesgos para abordar las consecuencias del empleo de las tecnologías de la información y las comunicaciones por los Estados, incluidos los intercambios de las opiniones nacionales sobre el empleo de esas tecnologías en los conflictos;

iii) Intercambiar información sobre la legislación nacional y las estrategias y tecnologías, políticas y mejores prácticas nacionales en cuanto a la seguridad de las tecnologías de la información y de las comunicaciones;

iv) Determinar qué medidas de apoyo a la creación de capacidad en los países menos adelantados podrían adoptarse;

v) Examinar las posibilidades de elaborar términos y definiciones comunes pertinentes con respecto a la resolución 64/25 de la Asamblea General.

Anexo

Lista de los miembros del Grupo de Expertos Gubernamentales sobre los avances en la información y las telecomunicaciones en el contexto de la seguridad internacional

Sr. Vladimir N. Gerasimovich
Jefe del Departamento de Seguridad Internacional y de Control de Armamentos
Ministerio de Relaciones Exteriores
Belarús

Sr. Aleksandr Ponomarev (tercer período de sesiones)
Consejero de la Misión Permanente de la República de Belarús ante la Oficina de las Naciones Unidas en Ginebra

Sr. Alexandre Mariano Feitosa
Comandante
Cuerpo de Marina Brasileño, Armada Brasileña
Secretaría de Políticas, Estrategias y Asuntos Internacionales
Ministerio de Defensa
Brasil

Sr. Li Song (períodos de sesiones primero y segundo)
Director General Adjunto
Departamento de Control de Armamentos y Desarme
Ministerio de Relaciones Exteriores
China

Sr. Kang Yong (períodos de sesiones tercero y cuarto)
Director General Adjunto
Departamento de Control de Armamentos y Desarme
Ministerio de Relaciones Exteriores
China

Sr. Linnar Viik
Profesor Adjunto
Colegio Superior Estoniano de Tecnología de la Información
Estonia

Sr. Aymeric Simon
Relations internationales
Agence nationale de la sécurité des systèmes d'information
Secrétariat général de la défense et de la sécurité nationale
Francia

Sr. Gregor Koebel
Jefe de la División de Control de Armas Convencionales
Oficina Federal de Relaciones Exteriores
Alemania

Sr. B. J. Srinath
Director Superior
Equipo Informático Indio de Respuesta en Casos de Emergencia
Departamento de Tecnología de la Información
India

Sra. Rodica Radian-Gordon
Directora
Departamento de Control de Armamentos
Ministerio de Relaciones Exteriores
Israel

Sr. Vincenzo Della Corte (períodos de sesiones primero y tercero)
Director del Sector de la Seguridad y las Comunicaciones
Presidencia del Consejo de Ministros
Italia

Sr. Walter Mecchia (períodos de sesiones segundo y cuarto)
Sector de Seguridad de las Comunicaciones
Presidencia del Consejo de Ministros
Italia

Sr. Rashid A. Al-Mohannadi (primer período de sesiones)
Comandante de la Compañía de Transmisiones de las Fuerzas Terrestres
Cuerpo de Transmisiones Amiri
Qatar

Sr. Saad M. R. Al-Kaabi
Teniente Coronel (Ingeniero)
Ministerio de Defensa
Qatar

Sr. Lew Kwang-chul
Embajador
Ministerio de Relaciones Exteriores y Comercio
República de Corea

Sr. Andrey V. Krutskikh
Director Adjunto
Departamento de Amenazas y Problemas Nuevos
Ministerio de Relaciones Exteriores
Federación de Rusia

Sra. Palesa Banda (primer período de sesiones)
Directora Adjunta, Gobernanza de Internet
Departamento de Comunicaciones
Sudáfrica

General de División Mario Silvino Brazzoli
Funcionario de Tecnología de la Información del gobierno
Departamento de Defensa
Sudáfrica

Sr. Gavin Willis
Equipo de Relaciones Internacionales
Organismo Técnico Nacional para la Seguridad de la Información (CESG)
Reino Unido de Gran Bretaña e Irlanda del Norte

Sr. Michele G. Markoff
Asesor de Categoría Superior en Materia de Políticas
Oficina de Asuntos Cibernéticos
Departamento de Estado de los Estados Unidos
Estados Unidos de América