



Asamblea General

Distr. general
24 de junio de 2013
Español
Original: inglés

Sexagésimo octavo 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 [66/24](#) de la Asamblea General.

* Publicado nuevamente por razones técnicas el 30 de julio de 2013.

** [A/68/150](#).



Informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional

Resumen

Las tecnologías de la información y las comunicaciones han transformado el panorama de la seguridad internacional. Esas tecnologías aportan unas ventajas económicas y sociales inmensas. Las tecnologías de la información y las comunicaciones también pueden utilizarse para fines contrarios a la paz y la seguridad internacionales, lo cual ha producido un aumento perceptible del riesgo en los últimos años, pues esas tecnologías se emplean con fines delictivos y para otras actividades de desestabilización. El uso de esas tecnologías con fines malintencionados por parte de agentes que, con frecuencia, actúan con impunidad es fácil de encubrir y puede ser difícil de atribuir a un autor concreto. Ello crea un entorno que facilita el empleo de las tecnologías de la información y las comunicaciones para empresas cada vez más sofisticadas.

Los Estados Miembros han afirmado con frecuencia la necesidad de colaborar en la lucha contra las amenazas derivadas del uso malicioso de las tecnologías de la información y las comunicaciones. La cooperación internacional es fundamental a fin de reducir los riesgos y mejorar la seguridad. Para que siga progresando la cooperación a nivel internacional, harán falta medidas destinadas a promover un entorno pacífico, seguro, abierto y cooperativo en las tecnologías de la información y las comunicaciones. Entre las medidas de cooperación que podrían aportar estabilidad y seguridad se cuentan las normas, las reglas y los principios de conducta responsable de los Estados, las medidas voluntarias para aumentar la transparencia y la confianza entre los Estados y las medidas de creación de capacidad. Los Estados deben asumir el liderazgo de esas iniciativas, pero una participación apropiada del sector privado y de la sociedad civil mejoraría la cooperación.

Habiendo reconocido la magnitud del problema, teniendo en cuenta las amenazas reales y potenciales, y basándose en las recomendaciones que figuran en el informe del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional de julio de 2010 ([A/65/201](#)), el Grupo de Expertos Gubernamentales ofrece en el presente informe sus recomendaciones para promover la paz y la estabilidad en el uso de las tecnologías de la información y las comunicaciones por parte de los Estados.

En el informe se reconoce que la aplicación de normas derivadas del derecho internacional vigente que sean pertinentes para el uso de las tecnologías de la información y las comunicaciones por parte de los Estados es esencial a fin de reducir los riesgos para la paz, la seguridad y la estabilidad internacionales. En el informe se recomienda que se continúe estudiando la cuestión a fin de promover un entendimiento común sobre la forma en que esas normas se aplican a la conducta de los Estados y al uso que estos hacen de las tecnologías de la información y las comunicaciones. Según se señala en el informe, dadas las singulares características de las tecnologías de la información y las comunicaciones con el tiempo podrían elaborarse normas adicionales.

El informe refleja la conclusión del Grupo de que el derecho internacional, y en particular la Carta de las Naciones Unidas, son aplicables y esenciales para mantener la paz y la estabilidad y para promover un entorno abierto, seguro, pacífico y accesible para las tecnologías de la información y las comunicaciones. El Grupo también concluyó que la soberanía del Estado y las normas y los principios internacionales que emanan de ella son aplicables a la realización de actividades relacionadas con las tecnologías de la información y las comunicaciones por parte de los Estados y a su jurisdicción sobre la infraestructura de tecnologías de la información y las comunicaciones dentro de su territorio; los Estados deben cumplir sus obligaciones internacionales en relación con los hechos internacionalmente ilícitos que se les puedan imputar. El informe contiene recomendaciones sobre la adopción de medidas voluntarias para incrementar la confianza y la transparencia, y también sobre la cooperación internacional para crear capacidad en la esfera de la seguridad de las tecnologías de la información y las comunicaciones, especialmente en los países en desarrollo. El Grupo recomienda celebrar con regularidad un diálogo institucional sobre estas cuestiones, bajo los auspicios de las Naciones Unidas, así como diálogos habituales en otros foros, con miras a fomentar esas medidas. Los Estados Miembros deberían estudiar seriamente el presente informe y valorar la forma de desarrollar y aplicar las recomendaciones que contiene.

Índice

	<i>Página</i>
Prólogo del Secretario General.	4
Carta de envío	5
I. Introducción.	6
II. Fomento de la cooperación para lograr un entorno pacífico, seguro, resistente y abierto para las tecnologías de la información y las comunicaciones	8
III. Recomendaciones sobre normas, reglas y principios de conducta estatal responsable	8
IV. Recomendaciones sobre medidas de fomento de la confianza y el intercambio de información	10
V. Recomendaciones sobre medidas de creación de capacidad	11
VI. Conclusión	12
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	13

Prólogo del Secretario General

Las tecnologías de la información y las comunicaciones están entrelazadas en la trama de la vida cotidiana. Si bien todos los países aprecian las enormes virtudes de estas tecnologías, también existe una amplia conciencia de que su uso indebido plantea riesgos para la paz y la seguridad internacionales.

En el presente informe se formulan recomendaciones preparadas por un grupo de expertos gubernamentales de 15 Estados para afrontar las amenazas existentes y las potenciales que se deriven del uso de las tecnologías de la información y las comunicaciones por Estados, agentes que actúen en nombre de Estados y agentes no estatales. Se basa en las recomendaciones formuladas en 2010 por un grupo de expertos anterior, que incluían la necesidad de seguir trabajando en normas, formas de aumentar la confianza y medidas para la creación de capacidad.

Aprecio que en el informe se destaquen la trascendencia de la Carta de las Naciones Unidas y el derecho internacional y la importancia de que los Estados se comporten con responsabilidad. Las recomendaciones señalan el camino para afianzar la seguridad de las tecnologías de la información y las comunicaciones en el marco del derecho internacional vigente y los entendimientos que rigen las relaciones entre los Estados y forman los cimientos de la paz y la seguridad internacionales.

Como señala el Grupo, las Naciones Unidas desempeñan una función importante en la promoción del diálogo entre sus Estados Miembros sobre la cuestión de la seguridad en el uso de las tecnologías de la información y las comunicaciones y el ulterior desarrollo de la cooperación internacional en esta esfera.

Quiero expresar mi agradecimiento a la Presidenta del Grupo y a los expertos por su diligente labor. El informe que elaboraron constituye una base sólida para futuras actividades dirigidas a mejorar la seguridad y la estabilidad en el uso de las tecnologías de la información y las comunicaciones. Encomio sus recomendaciones a la Asamblea General, que constituyen un avance crucial en la iniciativa mundial por minimizar los riesgos asociados a las tecnologías de la información y las comunicaciones y, al mismo tiempo, permitirán optimizar el valor de estas tecnologías.

Carta de envío

7 de junio de 2013

Tengo el honor de adjuntar a la presente 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 se estableció en 2012 en aplicación del párrafo 4 de la resolución 66/24 de la Asamblea General. Como Presidenta del Grupo, me complace señalar que el informe se aprobó por consenso.

En dicha resolución, titulada “Avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional”, la Asamblea General solicitó que en 2012 se estableciera un grupo de expertos gubernamentales sobre la base de una distribución geográfica equitativa para continuar examinando las amenazas reales y potenciales en la esfera de la seguridad de la información y las posibles medidas de cooperación para encararlas, como normas, reglas o principios de comportamiento responsable de los Estados y medidas de fomento de la confianza respecto del espacio informativo, así como los conceptos encaminados a fortalecer la seguridad de los sistemas mundiales de información y telecomunicaciones. Se pidió al Grupo que tuviese en cuenta las evaluaciones y recomendaciones que figuraban en el informe de un grupo anterior (A/65/201). Se solicitó al Secretario General que presentase un informe sobre los resultados de dicho examen a la Asamblea General en su sexagésimo octavo período de sesiones.

De conformidad con lo dispuesto en la resolución, se designó a expertos de 15 Estados: Alemania, Argentina, Australia, Belarús, Canadá, China, Egipto, Estados Unidos de América, Estonia, Francia, Federación de Rusia, India, Indonesia, Japón y Reino Unido de Gran Bretaña e Irlanda del Norte. La lista de expertos figura en el anexo.

En las reuniones del Grupo de Expertos Gubernamentales 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. El Grupo celebró tres períodos de sesiones: el primero, del 6 al 10 de agosto de 2012, en la Sede de las Naciones Unidas; el segundo, del 14 al 18 de enero de 2013, en Ginebra; y el tercero, del 3 al 7 de junio de 2013, en la Sede de las Naciones Unidas.

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 el Sr. James Lewis, la Sra. Kerstin Vignard (períodos de sesiones segundo y tercero) y el Sr. Ben Baseley-Walker (primer período de sesiones). El Grupo también desea dar las gracias al Sr. Ewen Buchanan, de la Oficina de las Naciones Unidas de Asuntos de Desarme, que se desempeñó como secretario del Grupo, y a otros funcionarios de la Secretaría que prestaron su asistencia al Grupo.

(Firmado) Deborah Stokes
Presidenta del Grupo

I. Introducción

1. El uso de las tecnologías de la información y las comunicaciones ha transformado el entorno de la seguridad internacional. Estas tecnologías aportan unas ventajas económicas y sociales inmensas, pero también pueden utilizarse para fines contrarios a la paz y la seguridad internacionales. Durante los últimos años se ha producido un aumento perceptible del uso de las tecnologías de la información y las comunicaciones con finalidades delictivas y de desestabilización.

2. La cooperación internacional es fundamental para reducir los riesgos y mejorar la seguridad. Por ese motivo, la Asamblea General solicitó al Secretario General que, con la asistencia de un grupo de expertos gubernamentales, continuase examinando las posibles medidas de cooperación para encarar las amenazas reales y potenciales y le presentase un informe al respecto en su sexagésimo octavo período de sesiones (resolución 66/24). El presente informe se basa en el informe de 2010 del Grupo de Expertos Gubernamentales anterior (A/65/201), que examinó esta cuestión y formuló recomendaciones acerca de las futuras labores conexas.

3. En el informe de 2010 se recomendó 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. Se pidió que se adoptasen medidas para fomentar la confianza y la estabilidad y reducir los riesgos, entre ellas el intercambio de opiniones nacionales sobre el uso de las tecnologías de la información y las comunicaciones en los conflictos, y se compartiese información sobre la legislación nacional y las estrategias, tecnologías, políticas y mejores prácticas nacionales en cuanto a la seguridad de las tecnologías de la información y las comunicaciones. En el informe de 2010 se destacó la importancia de crear capacidad en los Estados que pudiesen necesitar asistencia para abordar el problema de la seguridad de sus tecnologías de la información y las comunicaciones y se sugirió que se continuara trabajando para establecer términos y definiciones comunes.

4. Numerosas iniciativas bilaterales, regionales y multilaterales emprendidas desde 2010 han puesto de relieve que es cada vez más importante aumentar la seguridad de las tecnologías de la información y las comunicaciones y del uso de estas, reducir los riesgos para la seguridad pública, mejorar la seguridad de las naciones y afianzar la estabilidad mundial. Promover el uso de las tecnologías de la información y las comunicaciones con fines pacíficos redundaría en interés de todos los Estados. También interesa a los Estados prevenir conflictos derivados del uso de estas tecnologías. Llegar a un entendimiento común de las normas, reglas y principios aplicables al uso de las tecnologías de la información y las comunicaciones por los Estados y adoptar medidas voluntarias de fomento de la confianza puede ser importante para promover la paz y la seguridad. Aunque la labor de la comunidad internacional para encarar este desafío a la paz y la seguridad internacionales apenas ha comenzado, ya es posible formular una serie de medidas sobre normas, reglas y principios para una conducta estatal responsable.

Amenazas, riesgos y aspectos vulnerables

5. Las tecnologías de la información y las comunicaciones son de doble uso y pueden emplearse para fines tanto legítimos como malintencionados. Todos los

dispositivos de tecnologías de la información y las comunicaciones pueden ser el origen o el objetivo de usos indebidos. La utilización de las tecnologías de la información y las comunicaciones con fines malintencionados puede ser fácil de encubrir y difícil de atribuir a un autor concreto, lo que permite aprovecharlas de una manera sofisticada y, a menudo, con impunidad. La interconexión mundial de las redes de tecnologías de la información y las comunicaciones exacerba el problema. La combinación de la conectividad mundial, unas tecnologías vulnerables y el anonimato facilita el uso de las tecnologías de la información y las comunicaciones para realizar actividades desestabilizadoras.

6. Las amenazas a las personas, empresas, infraestructuras nacionales y gobiernos se han agravado, y los incidentes son cada vez más nocivos. Los orígenes de estas amenazas comprenden tanto agentes estatales como no estatales. Además, en la realización de actos indebidos con tecnologías de la información y las comunicaciones pueden intervenir particulares, grupos u organizaciones, incluidas organizaciones delictivas, que actúen por cuenta de Estados. La posibilidad de que agentes estatales y no estatales desarrollen y propaguen sofisticados instrumentos y técnicas maliciosas, como las redes zombi, puede intensificar el riesgo de que se produzca una atribución errónea o una escalada fortuita de la tensión. La falta de una interpretación común sobre lo que constituye una conducta estatal aceptable con respecto al uso de las tecnologías de la información y las comunicaciones hace aumentar los riesgos para la paz y la seguridad internacionales.

7. Los grupos terroristas utilizan las tecnologías de la información y las comunicaciones para comunicarse, recopilar información, reclutar adeptos, organizar, planificar y coordinar ataques, promover sus ideas y actividades, y recabar financiación. Si esos grupos consiguiesen instrumentos para llevar a cabo ataques, podrían emplear las tecnologías de la información y las comunicaciones para realizar actividades desestabilizadoras.

8. Los Estados están preocupados porque la integración de funciones dañinas ocultas en las tecnologías de la información y las comunicaciones podría aprovecharse de maneras que afectarían al uso seguro y fiable de estas tecnologías y la cadena de suministro de los productos y servicios de esta esfera, menoscabaran la confianza en el comercio y perjudicaran a la seguridad nacional.

9. El uso creciente de las tecnologías de la información y las comunicaciones en infraestructuras y sistemas de control industrial fundamentales genera nuevas posibilidades de desestabilización. El rápido aumento del uso de dispositivos de comunicaciones móviles, servicios web, redes sociales y servicios de computación en nube potencia los desafíos en el ámbito de la seguridad.

10. Las diferencias en los niveles de capacidad que tienen los Estados en la esfera de la seguridad de las tecnologías de la información y las comunicaciones pueden incrementar la vulnerabilidad en el mundo interconectado de hoy. Los agentes malintencionados explotan las redes con independencia de dónde se encuentren. Los aspectos vulnerables se amplifican a causa de las disparidades en las regulaciones, prácticas y legislaciones nacionales referentes al uso de las tecnologías de la información y las comunicaciones.

II. Fomento de la cooperación para lograr un entorno pacífico, seguro, resistente y abierto para las tecnologías de la información y las comunicaciones

11. Los Estados Miembros han afirmado reiteradamente la necesidad de cooperar en la lucha contra las amenazas derivadas del uso de las tecnologías de la información y las comunicaciones con fines malintencionados. A fin de progresar en la cooperación internacional será necesario adoptar una amplia variedad de medidas para promover un entorno pacífico, seguro, abierto y cooperativo para las tecnologías de la información y las comunicaciones. Deben examinarse medidas de cooperación que puedan contribuir a la paz, la estabilidad y la seguridad internacionales. Debe llegarse, por ejemplo, a un entendimiento común sobre cómo aplicar el derecho internacional pertinente y las normas, reglas y principios de conducta estatal responsable que se deriven de él.

12. Si bien los Estados deben liderar la labor destinada a afrontar estos desafíos, una participación apropiada del sector privado y la sociedad civil mejoraría la cooperación.

13. Las Naciones Unidas deberían desempeñar una función primordial en el fomento del diálogo entre los Estados Miembros para llegar a un entendimiento común sobre la seguridad de las tecnologías de la información y las comunicaciones y el uso de estas, alentar las iniciativas regionales, promover medidas de transparencia y fomento de la confianza y apoyar la creación de capacidad y la difusión de las mejores prácticas.

14. Además de las labores realizadas en el sistema de las Naciones Unidas, se están llevando a cabo iniciativas eficaces en organizaciones internacionales y entidades regionales como la Unión Africana, el Foro Regional de la Asociación de Naciones de Asia Sudoriental (ASEAN), el Foro de Cooperación Económica de Asia y el Pacífico, el Consejo de Europa, la Comunidad Económica de los Estados de África Occidental, la Unión Europea, la Liga de los Estados Árabes, la Organización de los Estados Americanos, la Organización para la Seguridad y la Cooperación en Europa (OSCE) y la Organización de Cooperación de Shanghai. Las labores futuras en la esfera de la seguridad del uso de las tecnologías de la información y las comunicaciones deberían tener en cuenta esas actividades.

15. Habiendo reconocido la magnitud de la problemática y teniendo en cuenta las amenazas reales y las potenciales, así como las recomendaciones que figuran en el informe de julio de 2010 del Grupo de Expertos Gubernamentales sobre los Avances en la Información y las Telecomunicaciones en el Contexto de la Seguridad Internacional ([A/65/201](#)), el Grupo recomienda las medidas que se relacionan a continuación.

III. Recomendaciones sobre normas, reglas y principios de conducta estatal responsable

16. La aplicación de normas derivadas del derecho internacional vigente que son pertinentes para el uso de las tecnologías de la información y las comunicaciones por los Estados es una medida fundamental con el fin de reducir los riesgos para la paz, la seguridad y la estabilidad internacionales. Es necesario continuar realizando

estudios para establecer un entendimiento común sobre cómo se aplicarán esas normas a la conducta estatal y el uso de las tecnologías de la información y las comunicaciones por los Estados. Dadas las singulares características de las tecnologías de la información y las comunicaciones, podrían elaborarse normas adicionales con el transcurso del tiempo.

17. El Grupo examinó las opiniones y observaciones sobre los avances en la esfera de la información y las telecomunicaciones en el contexto de la seguridad internacional comunicadas por los Estados Miembros en respuesta a la invitación que formuló la Asamblea General en sus resoluciones [64/25](#), [65/41](#) y [66/24](#), así como otras medidas que figuran en las resoluciones [55/63](#), [56/121](#), [57/239](#), [58/199](#) y [64/211](#).

18. El Grupo tomó nota del documento [A/66/359](#), difundido por el Secretario General a petición de los Representantes Permanentes de China, la Federación de Rusia, Tayikistán y Uzbekistán, que contenía el proyecto de código internacional de conducta para la seguridad de la información, posteriormente copatrocinado por Kazajstán y Kirguistán.

19. El derecho internacional, en particular la Carta de las Naciones Unidas, es aplicable y fundamental para mantener la paz y la estabilidad y fomentar un entorno abierto, seguro, pacífico y accesible en la esfera de esas tecnologías.

20. La soberanía de los Estados y las normas y principios internacionales que de ella emanan son aplicables a la realización de actividades relacionadas con las tecnologías de la información y las comunicaciones por los Estados y a su jurisdicción sobre la infraestructura de esas tecnologías que se halle en su territorio.

21. Las iniciativas de los Estados para ocuparse de la seguridad de las tecnologías de la información y las comunicaciones deben ir de la mano del respeto de los derechos humanos y las libertades fundamentales enunciados en la Declaración Universal de los Derechos Humanos y otros instrumentos internacionales.

22. Los Estados deberían intensificar la cooperación en la lucha contra el uso de las tecnologías de la información y las comunicaciones con fines delictivos o de terrorismo, armonizar los enfoques jurídicos de la manera apropiada y fortalecer la colaboración práctica entre sus respectivos organismos de seguridad y fiscalías.

23. Los Estados deben cumplir sus obligaciones internacionales en lo que respecta a los hechos internacionalmente ilícitos que se les puedan atribuir. Los Estados no deben valerse de agentes que cometan esos hechos por cuenta de ellos. Los Estados deben asegurarse de que su territorio no sea utilizado por agentes no estatales para hacer un uso ilícito de las tecnologías de la información y las comunicaciones.

24. Los Estados deberían alentar al sector privado y la sociedad civil a contribuir de manera apropiada a mejorar la seguridad de las tecnologías de la información y las comunicaciones y de su uso, incluida la seguridad de la cadena de suministro de productos y servicios de las tecnologías de la información y las comunicaciones.

25. Los Estados Miembros deberían examinar cuál es la mejor forma de cooperar para aplicar las normas y principios de conducta responsable antes señalados, incluida la función que podrían asumir el sector privado y las organizaciones de la sociedad civil. Esas normas y principios complementan la labor de las Naciones Unidas y los grupos regionales y forman la base para adoptar otras medidas de fomento de la confianza.

IV. Recomendaciones sobre medidas de fomento de la confianza y el intercambio de información

26. Las medidas voluntarias de fomento de la confianza pueden promover la tranquilidad y la confianza entre los Estados y ayudar a reducir el riesgo de conflictos al aumentar la previsibilidad y reducir las percepciones erróneas. Pueden contribuir considerablemente a despejar las inquietudes de los Estados sobre el uso de las tecnologías de la información y las comunicaciones por los Estados y podrían constituir un avance significativo hacia una mayor seguridad internacional. Los Estados deben estudiar la posibilidad de formular medidas prácticas de fomento de la confianza de cara a incrementar la transparencia, la previsibilidad y la cooperación, entre ellas:

a) El intercambio voluntario de opiniones e información sobre políticas y estrategias nacionales, mejores prácticas, procesos de toma de decisiones, organizaciones nacionales competentes y medidas para mejorar la cooperación internacional. Los Estados que proporcionen información determinarán cuál será el alcance de esta, que podría compartirse de manera bilateral y en grupos regionales u otros foros internacionales;

b) La creación de marcos consultivos bilaterales, regionales y multilaterales para el fomento de la confianza, que podrían consistir en talleres, seminarios y ejercicios para afinar las deliberaciones nacionales sobre cómo prevenir incidentes desestabilizadores derivados del uso estatal de las tecnologías de la información y las comunicaciones, y de qué manera podrían surgir y afrontarse esos incidentes;

c) El perfeccionamiento del intercambio de información entre Estados sobre incidentes de seguridad en la esfera de las tecnologías de la información y las comunicaciones mediante un uso más eficaz de los canales existentes o la creación de nuevos canales y mecanismos apropiados para recibir, recopilar, analizar e intercambiar información sobre incidentes relativos a las tecnologías de la información y las comunicaciones, para que sea posible adoptar medidas de respuesta, recuperación y mitigación oportunamente. Los Estados deberían considerar la posibilidad de intercambiar información sobre puntos de contacto nacionales a fin de ampliar y mejorar los canales de comunicación existentes para la gestión de situaciones de crisis y apoyar la creación de mecanismos de alerta temprana;

d) Los intercambios bilaterales de información y la comunicación entre los equipos nacionales de respuesta a emergencias cibernéticas, entre las comunidades de este tipo de equipos y en otros foros, para contribuir al diálogo a nivel político y de formulación de políticas;

e) Una mayor cooperación para afrontar los incidentes que pudieran afectar a la infraestructura informática o a las infraestructuras fundamentales que dependan de sistemas de control industrial basados en tecnologías de la información y las comunicaciones. Esta cooperación podría incluir directrices y mejores prácticas de cooperación interestatal contra tentativas de desestabilización perpetradas por agentes no estatales;

f) El perfeccionamiento de los mecanismos de cooperación entre organismos de seguridad para reducir los incidentes que pudieran malinterpretarse como acciones estatales hostiles, con el fin de mejorar la seguridad internacional.

27. Estas actividades iniciales de fomento de la confianza pueden ofrecer una experiencia práctica y servir de orientación para futuras labores. Los Estados deberían alentar y aprovechar los progresos realizados de manera bilateral y multilateral, incluidos los registrados en grupos regionales como la Unión Africana, el Foro Regional de la ASEAN, la Unión Europea, la Liga de los Estados Árabes, la Organización de los Estados Americanos, la OSCE, la Organización de Cooperación de Shanghai y otros. Tomando como base esas actividades, los Estados deberían procurar que las medidas adoptadas fuesen complementarias y facilitar la difusión de las mejores prácticas, teniendo en cuenta las diferencias entre distintas naciones y regiones.

28. Los Estados deben liderar la preparación de medidas de fomento de la confianza, pero una contribución apropiada del sector privado y la sociedad civil redundaría en beneficio de esa labor.

29. Dada la velocidad a que evolucionan las tecnologías de la información y las comunicaciones y el alcance de la amenaza, el Grupo juzga necesario afianzar el entendimiento común e intensificar la cooperación práctica. En este sentido, el Grupo recomienda que se celebre con regularidad un diálogo institucional con una amplia participación bajo los auspicios de las Naciones Unidas y diálogos en foros bilaterales, regionales y multilaterales y otras organizaciones internacionales.

V. Recomendaciones sobre medidas de creación de capacidad

30. La creación de capacidad tiene una importancia vital de cara a la efectividad de la cooperación mundial sobre la seguridad de las tecnologías de la información y las comunicaciones y su uso. Algunos Estados pueden necesitar ayuda para mejorar la seguridad de sus infraestructuras fundamentales de tecnologías de la información y las comunicaciones; desarrollar su pericia técnica y preparar leyes, estrategias y marcos reguladores apropiados para cumplir sus responsabilidades; y salvar las diferencias de seguridad de las tecnologías de la información y las comunicaciones y su uso.

31. En este sentido, los Estados que colaboren con organizaciones internacionales, incluidos los organismos de las Naciones Unidas, y el sector privado deberían estudiar cuál es la mejor forma de ofrecer asistencia técnica y de otro tipo para crear capacidad en materia de seguridad de las tecnologías de la información y las comunicaciones y su uso a los países que necesiten ayuda, en especial los países en desarrollo.

32. Tomando como base la labor realizada en la preparación de anteriores resoluciones e informes de las Naciones Unidas sobre el fomento de la capacidad, como la resolución [64/211](#) de la Asamblea General, los Estados deberían estudiar la posibilidad de adoptar las medidas siguientes:

a) Apoyar las actividades bilaterales, regionales, multilaterales e internacionales de fomento de la capacidad para hacer más seguras las infraestructuras y el uso de las tecnologías de la información y las comunicaciones; fortalecer los marcos jurídicos y la capacidad y las estrategias de las fuerzas del orden a nivel nacional; combatir el uso de las tecnologías de la información y las

comunicaciones con fines delictivos y terroristas; y ayudar a identificar y difundir las mejores prácticas;

b) Crear y fortalecer la capacidad de respuesta a incidentes, incluidos los equipos de respuesta a emergencias cibernéticas, y fortalecer la cooperación entre equipos de este tipo;

c) Apoyar el desarrollo y la utilización del aprendizaje electrónico, la formación y la sensibilización con respecto a la seguridad en la esfera de las tecnologías de la información y las comunicaciones para contribuir a superar la brecha digital y ayudar a los países en desarrollo a mantenerse al día de las novedades en materia de políticas que se registren a nivel internacional en esta esfera;

d) Intensificar la cooperación y la transferencia de conocimientos y tecnologías para gestionar los incidentes de seguridad relacionados con las tecnologías de la información y las comunicaciones, especialmente en favor de los países en desarrollo;

e) Alentar a los institutos de investigación y las universidades a que prosigan el análisis y el estudio de cuestiones relacionadas con la seguridad de las tecnologías de la información y las comunicaciones. Dado que tienen el mandato específico de apoyar a los Estados Miembros de las Naciones Unidas y la comunidad internacional, los Estados deben estudiar qué función pueden desempeñar en este sentido los institutos pertinentes de investigación y formación de las Naciones Unidas.

33. El Grupo reconoció que los avances en la seguridad del uso de las tecnologías de la información y las comunicaciones, entre otras vías mediante el fomento de la capacidad, contribuirían también a la consecución del octavo Objetivo de Desarrollo del Milenio, “fomentar una asociación mundial para el desarrollo”.

VI. Conclusión

34. El progreso en el ámbito de la seguridad internacional en el uso de las tecnologías de la información y las comunicaciones por los Estados será iterativo: cada paso del camino partirá del anterior. Este enfoque será necesario porque el entorno tecnológico está configurado por el cambio y por el crecimiento constante del número de usuarios de las tecnologías de la información y las comunicaciones. En el presente informe se formulan recomendaciones que se basan en trabajos anteriores. Su aplicación y su perfeccionamiento contribuirán a aumentar la confianza entre todas las partes interesadas. El Grupo recomienda que los Estados Miembros estudien seriamente el presente informe y valoren la forma de desarrollar y aplicar estas recomendaciones.

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****Alemania**

Sr. Detlev Wolter

Jefe de la Dirección de control de armas convencionales y medidas de fomento de la confianza y la seguridad, Oficina Federal de Relaciones Exteriores, Berlín

Argentina

Embajador Alfredo Morelli

Director del Grupo Especial de Asuntos Tecnológicos del Ministerio de Relaciones Exteriores y Culto, Buenos Aires

Australia

Sra. Deborah Stokes

Primera Secretaria Adjunta del Ministerio de Relaciones Exteriores y Comercio, Canberra

Belarús

Sr. Vladimir N. Gerasimovich

Jefe del Departamento de Seguridad Internacional y de Control de Armamentos del Ministerio de Relaciones Exteriores, Minsk

Canadá

Sr. Michael Walma

Director de la División de Planificación de Políticas, Departamento de Relaciones Exteriores y Comercio Internacional, Ottawa

China

Sr. Lei Wang (períodos de sesiones primero y segundo)

Director del Departamento de Control de Armas y Desarme del Ministerio de Relaciones Exteriores, Beijing

Sra. Zhihua Dong (tercer período de sesiones)

Consejera del Departamento de Control de Armas y Desarme del Ministerio de Relaciones Exteriores, Beijing

Egipto

Dr. Sherif Hashem

Asesor Superior para seguridad cibernética del Ministerio de Comunicaciones y Tecnología de la Información, Ministerio de Comunicaciones y Tecnología de la Información, el Cairo

Estados Unidos de América

Sra. Michele G. Markoff

Coordinadora Adjunta para cuestiones de tecnologías de la información y las comunicaciones de la Oficina del Secretario de Estado, Departamento de Estado, Washington, D.C.

Estonia

Sr. Linnar Viik

Director interino del Colegio Superior Estonio de Tecnología de la Información, Tallin

Federación de Rusia

Andrey V. Krutskikh

Coordinador Especial para asuntos políticos en relación con el uso de las tecnologías de la información y las comunicaciones, Embajador en Misión Especial, Ministerio de Relaciones Exteriores, Moscú

Francia

Sr. Jean-François Blarel

Vicesecretario General y Coordinador para asuntos cibernéticos del Ministerio de Relaciones Exteriores, París

India

Sr. Harsh K. Jain

Secretario Conjunto y Jefe de la División de Gobernanza Electrónica y Tecnología de la Información del Ministerio de Relaciones Exteriores, Nueva Delhi

Indonesia

Sr. Febrian A. Ruddyard (primer período de sesiones)

Director de Seguridad Internacional y Desarme del Ministerio de Relaciones Exteriores, Yakarta

Sr. Andy Rachmianto (tercer período de sesiones)

Ministro Consejero de la Misión Permanente de Indonesia ante las Naciones Unidas, Nueva York

Japón

Embajador Tamotsu Shinotsuka (primer período de sesiones)

Cooperación Internacional contra el Terrorismo, Política sobre Asuntos Cibernéticos y Delincuencia Organizada Internacional, Ministerio de Relaciones Exteriores, Tokio

Embajador Osamu Imai (períodos de sesiones segundo y tercero)

Cooperación Internacional contra el Terrorismo, Política sobre Asuntos Cibernéticos y Delincuencia Organizada Internacional, Ministerio de Relaciones Exteriores, Tokio

Reino Unido de Gran Bretaña e Irlanda del Norte

Sr. Nicholas Haycock

Director Adjunto de Seguridad Internacional, Oficina de Seguridad Cibernética y de Comunicaciones y Seguridad de la Información, Oficina del Gabinete, Londres
