CARI / CONSEJO ARGENTINO PARA LAS RELACIONES INTERNACIONALES

Las opiniones expresadas en esta publicación son exclusiva responsabilidad de sus autores y no reflejan necesariamente el pensamiento del CARI.

1

GRUPO DE TRABAJO SOBRE LA INSERCIÓN DE LA ARGENTINA EN EL MUNDO

Apuntes para una charla sobre la administración del conflicto internacional en el ciberespacio*

Alfredo Morelli **

El 6 de Septiembre de 2007, Israel bombardeó un centro de investigaciones nucleares construido por Corea del Norte en Siria que había gastado millones en un sistema de defensa antiaérea comprado a Rusia. La Fuerza Aérea de Israel entró al espacio aéreo sirio con aviones comunes sin que el sistema de defensa avisara.

Este es un ejemplo de ciber guerra: son acciones de un estado para entrar en los sistemas de otro con la intención de causar daño o disrupciones; en vez de bombardear las defensas del espacio aéreo, las inutilizan.

Hace más de 20 años que Estados Unidos incorporó esta tecnología con aplicaciones militares. En 1990 en la primera guerra de Irak, le ofrecen al Comandante, Gral. Norman Swchwarzkof, la posibilidad de deshabilitar las defensa iraquíes con armas cibernéticas; como buen soldado tradicional que era, prefirió bombardear, probablemente con mayor costo de vidas y equipamiento. En la segunda guerra de Irak, las fuerzas armadas estadounidenses utilizaron el correo electrónico para acción psicológica.

Vemos dos formas de usar la tecnología para acciones militares, en el caso de Siria para facilitar la guerra convencional y en Irak para propaganda y acción psicológica.

En Abril del 2007 ocurre el ataque a Estonia - aparentemente fue una reacción de hackers patrióticos rusos ante la remoción del monumento al soldado soviético en la ciudad de Tallin. Por varios días los servicios bancarios y los sitios gubernamentales se vieron afectados.

En 2008 Rusia invade Georgia y se atacan los medios de comunicación georgianos para desinformar a la población. También sufren los sistemas bancarios.

En el año 2010 la International Atomic Energy Agency (IAEA) completó la inspección de la planta de enriquecimiento de Natanz (Irán). Teherán reemplaza por año aproximadamente el 10% de las 8.700 centrifugadoras que tienen. Unas 800 por año que cuando salen de servicio deben ser inspeccionadas. Cuando de regreso en Viena revisan las filmaciones los inspectores se dan cuenta que Irán esta reemplazando un número mucho mayor que podría llegar a 1000 centrifugadoras. Con posterioridad se supo que en el año 2009 la planta de enriquecimiento había sido inoculada con un virus, descubierto por Ralph Langer, que se conoció como Stuxnex, el más potente hasta ese momento cuyo efecto fue poner fuera de control a las centrifugadoras que funcionaban con un software de control diseñado y provisto por Simens.

Hay muchos casos del uso de las Tecnologías de la información y de la Comunicación para producir efectos nocivos en los sistemas de otros países y empresas. Muchos casos quedan sin conocerse ya que aquellos que sufren los ataques prefieren ser discretos que permita evitar daños adicionales al prestigio de su negocio, como podría ser el caso de la actividad bancaria.

El ciberespacio. Definición y características

La teoría de juegos ofrece una herramienta útil para comprender la complejidad conceptual de una cuestión. La posibilidad de identificar el número de actores y la cantidad de cuestiones sobre las que los actores interactúan es irremplazable a la hora de entender los intereses y las fuerzas que dan forma a una realidad. Como puede verse en el anexo 2 la cuestión “Ciber” es de una extraordinaria complejidad, por la arquitectura necesaria para su funcionamiento, por la cantidad de “cosas” que ocurren en el espacio cibernético, y por la cantidad de sistemas integrados al mismo.

Trataré de dar un pantallazo de algunas cuestiones e interrogantes que se plantean, con la advertencia de que es un área de mucha novedad, de gran precariedad conceptual y de cambios permanentes. Lo que se dice siempre está en borrador.

¿Qué es el ciberespacio?

El ciberespacio está formado por todas las redes de computación y todo lo que conecta y controla. Internet es una red de redes, abierta. El ciberespacio incluye Internet, más otras redes que no son abiertas; es el espacio en el que la información digitalizada se comunica por medio de computadoras.

Si tuviéramos que dar una definición militar, diría que es el dominio caracterizado por el uso de medios electrónicos y el espectro electromagnético para guardar, modificar e intercambiar información vía sistemas en red.

Ahora bien, es tentador considerar al ciberespacio como otro “dominio” como hacemos con aire, tierra, mar o espacio y esto es un error. El ciberespacio es diferente se parece más a universos paralelos invisibles y misteriosos pero que afectan al mundo real.

---

* El autor agradece la colaboración de Luis Arregui, Carlos Escudé, Olga Cavalli y Raúl Palenque.

**Embajador Alfredo Morelli / Participó como experto argentino en el Grupo de Expertos Gubernamentales nombrado por el Secretario General de Naciones Unidas en 2012-2013

Alfredo Morelli / Apuntes para una charla sobre la administración del conflicto internacional en el ciberespacio

2

El mundo ocurre en el ciberespacio; es trasversal a todos los aspectos de la vida humana, desde la política, la economía, el esparcimiento; el ciberespacio está modificando la forma en que los seres humanos se comunican, se informan, se relacionan, negocian, innovan, e incluso piensan (1). Millones de transacciones se realizan por segundo. El sinnúmero de actores esta formado por estados, desarrolladores de aplicaciones, proveedores de contenido, proveedores de la infraestructura, la empresas como Google, Yahoo, agencias técnicas, agencias de estándares, fabricantes de equipos electrónicos, proveedores de seguridad, bancos, comerciantes, delincuentes, terroristas, individuos a través de las redes sociales.

El ciberespacio está compuesto también por otras redes que supuestamente no son accesibles por Internet. (no conectadas a la red o separadas por un "air gap") Redes que controlan otros sistemas, como gasoductos, oleoductos, centrales de energía, ferrocarriles, control de navegación aérea, sistemas portuarios, sistemas de control de importaciones y exportaciones, registros impositivos. Más recientemente con lo que se llama "el Internet de las cosas" hay un sinnúmero de "gadgets" electrodomésticos, ascensores, fotocopiadoras, ascensores, automóviles y hasta aparatos médicos, como una marcapasos, que funcionan y son controlados "en red".

El conflicto en el ciberespacio

Defino conflicto en un sentido amplio que incluye la ciber penetración de una red ajena, como el ciber ataque y el ciber crimen. Es interesante destacar que la mayor parte de los especialistas que tratan la guerra no tratan el crimen, lo que se justifica por la naturaleza militar de uno y judicial policial del otro. Como consecuencia, en la mayor parte de los casos dependen de Agencias Gubernamentales que no tienen contacto entre ellas (2). Creo que es un error porque hay mucha interacción entre guerreros y delincuentes cuyos roles y desarrollos se intercambian con frecuencia.

Internet tiene una estructura institucional multiparticipativa (multistakeholder) que por su naturaleza es proclive al conflicto. Los actores del ciberspacio son los Estados, las empresas, la sociedad civil entre los que se incluye a terroristas, ciber activistas o ciber criminales, dependiendo del código penal que miremos.

Los actores se definen o califican en relación al objetivo de sus acciones disruptivas: ciber delincuente, ciber terrorista, ciber guerrero o ciber espía. Los actores estatales pueden actuar por sí mismos o por interpósita persona haciendo uso de un actor no estatal como Proxy. Esta variedad de actores estatales y no estatales en un mismo escenario es una característica de cuidado porque en caso de situaciones militares o diplomáticas los actores privados podrían desestabilizar las interacciones gubernamentales y no sabríamos quién actúa por quién (3).

El ciber guerrero o el hacker con motivaciones diversas, en teoría pueden ingresar en cualquier red. Una vez "adentro" pueden controlar el sistema, robar información, modificarla, dar directivas para transacciones, derramar petróleo, descarrilar un tren, chocar aviones, desviar un misil, mover satélites, producir apagones. Frente a esto es muy difícil defenderse, lo que primero busca la víctima es restaurar las funciones de su sistema lo antes posible.

También calificamos al actor como ciber guerrero o ciber criminal dependiendo de para quien trabaje. El delito en red es el sector de mayor crecimiento de la economía mundial; hay tan poca persecución y es tan inefectiva que parece que de facto estuviera permitida, de hecho es un importante factor de riesgo para los gobiernos. (4)

La ciber seguridad

La ciber seguridad consiste en medidas para proteger el funcionamiento de una computadora o la información que contiene de una acción hostil.

¿Por qué hay fallas que permiten que se pueda entrar en las redes?

1. Hay fallas en el diseño de Internet. Internet no fue hecho para ser seguro. Los creadores de Internet eran contraculturales, si bien buscaban un sistema de control militar. Hubo mucha buena fe por parte de sus creadores, como ocurrió con otros casos de desarrollos científicos con aplicaciones militares. Hubo después alguna desilusión y la sensación de haber creado un monstruo.
2. Fallas en el hardware y en el software, porque se privilegia la funcionalidad de la aplicación y no los elementos de seguridad.
3. Hay muchos más sistemas "en red" con lo que aumentan los posibles blancos de ataque y las vulnerabilidades.

Con la globalización, la cadena de proveedores se amplía a muchos actores y aumentan las oportunidades de plantar un virus u otros elementos que generen vulnerabilidades futuras.

Las cuestiones que plantea el ciberespacio

Además de su vulnerabilidad, el ciberespacio tiene particularidades que hacen singularísimo al conflicto en ese ambiente. No es posible migrar ejemplos de estrategias provenientes de otros sistemas de armas como podrían ser las químicas, bacteriológicas o nucleares.

Ataque

La Carta de las UN en el Art. 2 inciso 4 dice: que los miembros *"se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier estado"*.

No hay acuerdo sobre qué incidente cibernético constituye uso de la fuerza.

Para Occidente, es cualquier acción dirigida a afectar las funciones de una red de computadoras por razones políticas o de seguridad nacional. Puede ser mediante una denegación de servicio, mediante la colocación de información falsa, o por la infiltración de una red protegida.

Un ciber ataque es la penetración no autorizada por un gobierno en los sistemas o redes de otro, o cualquier otra actividad, que puede ser cinética, que afecta un sistema y cuyo propósito es agregar, alterar, falsificar datos o producir la disrupción del sistema.

El objetivo de una acción la define como guerra, terrorismo o delito. Es guerra cuando actor es un estado y el objetivo es la "Seguridad Nacional", este objetivo político la distingue del ciber crimen, llevado a cabo por un actor no estatal por razones de ganancia económica. El terrorismo es un ataque llevado a cabo por un actor no estatal con motivaciones políticas. El espionaje no es un ataque porque no altera información.

Para los países del Grupo de Shangai, China, Rusia, Kazajistán, Kirgistán, Tayikistán y Uzbekistán así como para otros países como India o Bielorrusia un ciber ataque es además, "el uso de la información con el objetivo de afectar la estabilidad política".

No existe consenso sobre qué clase de ataque cibernético es equiparable a un ataque armado y constituye un

"acto de guerra" que justifique una respuesta basada en el derecho a la legítima defensa. En efecto, el Art. 51 de la Carta de las Naciones Unidas lee*: "Ninguna disposición de esta Carta menoscabará el derecho inmanente de legítima defensa, individual o colectiva, en caso de ataque armado contra un miembro de las Naciones Unidas, hasta tanto el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales"*.

Si bien el espionaje no es un acto de guerra y no está prohibido por el Derecho Internacional, el umbral entre el espionaje y lo que puede ser un acto de guerra es muy difuso. Se puede entrar en una red ajena con el objetivo de espiar o para preparar el campo de batalla; colocar vulnerabilidades en el sistema para ser usados en algún momento, ya sea inmediato o en el futuro. La colocación de fallas en sistemas ajenos puede ser indicio de un ataque, pero no indica su inminencia. Se producen un sinnúmero de incidentes por semana entre Estados Unidos y China para probar vulnerabilidades, pero lo difícil es entender su significado en términos de la inminencia de un ataque. (5)

Si bien hay numerosos incidentes la mayoría de ellos no llegan al nivel de justificar una respuesta cinética y no se producen en el contexto de un conflicto. La realidad es que por la indefinición y la incertidumbre los estados son muy discretos con relación a informar habar sido víctimas de un ataque e con las respuestas dadas.

Todo este terreno es muy confuso, si bien el objetivo califica a un ciber ataque como guerra o crimen, la magnitud del daño ocasionado también podría definirlo. Si los hackers roban del Banco Nacional de un país un millón de dólares, es un delito pero si roban las reservas de un Banco Central, afectarían la seguridad nacional del estado.

Atribución

En mi criterio lo que define la naturaleza excepcional del conflicto en el ciberespacio es la imposibilidad de atribuir el ataque a un autor determinado. Esta característica condiciona toda especulación que podamos hacer sobre una posible estrategia de manejo del conflicto en el ciberespacio. Esto se agrava con el uso de proxis, cualquier persona disgustada con medidas tomadas por un país determinado lanza un ataque contra ese país. Es lo que parece haber sucedido en Estonia cuando cambiaron de lugar la estatua del soldado soviético, hackers patrióticos lanzaron un ataque contra los servicios públicos. Las reacciones primeras atribuían el ataque a hackers patrióticos de Rusia, también se especuló con la participación de los servicios de inteligencia, que usando agentes intermediarios manifestaron su desagrado. Este ataque fue iniciado en la misma Estonia.

Es imposible saber quién realizó un ataque, hay varias dificultades una cuestión es encontrar la máquina, la dirección IP de la salió el ataque, en qué lugar, podemos conocer de quién era la propiedad, pero no sabemos qué persona apretó la tecla, ni tampoco si no era una máquina zombie que recibía ordenes de otro lado. Un ataque puede ser iniciado a dos cuadras de la Casa Blanca y aparecer como iniciado en Rusia, China, Yemen o Cuba. Aquí el tiempo es crucial, si es un ataque militar, la respuesta debería ser inmediata y cómo es muy difícil saber quién inició el ataque los riesgos son enormes. Los especialistas reconocen que resolver la atribución es el problema más difícil que encuentran. (6)

La disuasión

Frente al dilema de la administración del conflicto en el ciberespacio lo primero que uno piensa es sobre la lógica que hace que los estados se abstengan de usar su arsenal de armas cibernéticas. Inmediatamente surge la idea de una estrategia de disuasión: una defensa creíble es el primer objetivo de la estrategia, pero en el ciber espacio el ataque no es necesariamente una buena defensa. Por ello no está desarrollada la lógica de la disuasión. Esta debiera basarse en capacidades demostradas, en los efectos creíbles de las armas cibernéticas, en el efecto demostración, que no tienen, porque por un lado estas capacidades son secretas, ya que los desarrollos se usan una vez y se copian. Una vez usado, el arsenal desaparece y uno no sabe qué se encuentra del otro lado. Las defensas que uno tenía planeadas pueden haber sido deshabilitadas de antemano por el adversario que las descubrió sin que nos percatáramos de ello.

Tomemos como ejemplo el caso del virus Stuxnet. Estados Unidos tal vez cometió un error al lanzar el ataque porque si bien puede haber atrasado el programa nuclear iraní, el desarrollo ahora está en manos de los ciber guerreros o delincuentes de todo el mundo que podrían usarla para atacar las propias redes norteamericanas. (7)

De hecho el propio Stuxnet evolucionó en la web hacia versiones más sofisticadas y dañinas primero como Duku y luego como Flame.

Es la capacidad potencial de sorprendernos que tengan las defensas de un oponente la que hace a la disuasión cibernética diferente de la nuclear, que no es transferible. El *"first use"* tampoco sirve. Por otra parte, la disuasión está condicionada por las dificultades en la atribución de un ataque. No es casual que León Panetta, cuando estaba a cargo de Departamento de Defensa insistiera mucho en los progresos que su oficina había logrado en identificar los orígenes del ataque. (8)

Para complicar más la cuestión está la naturaleza dual de la tecnología. La proliferación cibernética y el desarrollo de capacidades en el ciberespacio son buscadas y deseadas por su efecto benéfico en el desarrollo. Reducir la brecha digital es un objetivo político y de desarrollo humano que está entre los objetivos del milenio. El número de actores es infinitamente mayor que en cualquier otro de los dominios en los que la guerra es posible con lo que una estrategia basada en el control de los actores o la proliferación de la tecnología es imposible.

Por otra parte, los Estados se cuidan de definir "líneas rojas" de advertencia porque creen que esto incitaría a operaciones menores. La posibilidad más que la certidumbre de la represalia es lo único que hace pensar dos veces al que podría atacar antes de hacerlo.

Control

La cuestión del Control es fundamental en la guerra. ¿Quién tiene la autoridad de penetrar una red extranjera y usar armas cibernéticas? En otros dominios la cadena de mandos está perfectamente establecida y hay mecanismos para evitar usos no autorizados del arma de que se trate. En este caso hay mucha ambigüedad. Es de por sí complicado integrar a los Cyber punks o nerds a la estructura militar, a la cultura del secreto y de la verticalidad. Además hay una barrera técnica (al menos por un par de generaciones) a la com-

prensión de los algoritmos o las aplicaciones de un arma cibernética.

La diferencia entre entrar en un sistema para espiar, para conocerlo o para dejarlo sin funcionar es apretar un par de teclas. Así, con un par de teclas más, podemos desatar una guerra. El Secretario Kerry refiriéndose al espionaje que la Agencia Nacional de Seguridad realizó sobre algunos líderes políticos, entre ellos Angela Merkel, usó la frase "piloto automático" al referirse "because the technology is there and the ability is there" Esto no es más que una muestra de las dificultades del control. (9)

El Control es difícil; no es como en lo nuclear en que el Presidente de los Estados Unidos viaja con la valija, las llaves y la clave. Aquí cualquiera puede entrar sin autorización o con una percepción vaga de que tenía la autorización. (10)

La paradoja de las capacidades en el ciberespacio

Paradojalmente, los países más avanzados son los más vulnerables porque tienen más sistemas en red. No importa la capacidad propia, siempre pueden hacer más, es algo paralizante incluso para la guerra convencional si un país tiene más sistemas de armas dependientes de lo ciber.

Para la propia República Argentina la implementación del plan Argentina Conectada a la par de reducir la brecha digital aumentará su vulnerabilidad. La propia naturaleza dual de la tecnología hace complicada la respuesta. El desarrollo de capacidades en el ciberespacio es positivo para un país pero también lo hace vulnerable. Cuando la tecnología es dual, no son verificables los límites. Las asimetrías juegan a favor del más débil que con poco puede hacer mucho.

Si analizamos por ejemplo el caso de los Estados Unidos, vemos que tiene poca infraestructura estatal- la mayor parte de la infraestructura crítica es de propiedad privada, de un sector privado con mucho poder de lobby que logra permanecer sin ser regulado. Este sector privado formula una ecuación de seguridad diferente de la que hace el Gobierno. Es curioso que en esta materia, la responsabilidad del estado por proveer la defensa nacional, no aplique a la infraestructura privada.

En una guerra convencional "proveer a la defensa nacional" incluye las industrias, cualquiera ellas sean; en el caso de la seguridad del ciberespacio, la infraestructura crítica privada tiene defensas más débiles porque la ecuación costo-beneficio que hace la empresa privada es diferente.

Estados Unidos tiene Fuerzas Armadas muy "red céntricas" y mucha dependencia de los contratistas privados, lo que genera enormes vulnerabilidades por las dificultades de generar una cultura de seguridad en la gran cantidad de personal civil que trabaja en temas del ciberespacio. La historia de Edward Snowden no es más que una muestra de estas dificultades.

Si hiciéramos un cuadro de fortaleza general, considerando la capacidad ofensiva, la defensiva y la dependencia, Corea del Norte, China y Rusia son más fuertes que los Estados Unidos. Cuanta más "en red" hay, mayor su dependencia. Es bueno estar conectado pero aumenta su vulnerabilidad. Haciendo esos cálculos se mide la fortaleza para la guerra cibernética. EEUU tiene 11 puntos, Rusia 16, China 15, Irán 12 y Corea del Norte 18*)* (11).

Considerando su vulnerabilidad, podría pensarse que a los Estados Unidos le interesaría un acuerdo. Pero la experiencia de los procesos de desarme no es muy alentadora. Los países colocan sobre la mesa lo que de todas maneras pensaban eliminar o aceptan límites que ya estaban en sus planes de desarrollo. El desarme no evitó que Israel, Pakistán, India, Africa del Sur, Corea del Norte adquirieran armas nucleares. En armas biológicas la URSS tuvo un arsenal oculto hasta hace poco tiempo. Las armas químicas se usaron en Vietnam, Falluja, Afganistán y Siria. Es difícil generar legitimidad cuando las dos superpotencias invitan a participar. Los dos prohíben a terceros adquirir armas nucleares, con una vaga promesa de reciprocidad.

Un test para determinar el interés sobre el control de armas cibernéticas es ver si los países están dispuestos a limitar las inversiones en el tema, cosa que no sucede, sino todo lo contrario. Intentar controlar, puede ser una estrategia para frenar al adversario en un área en la que estiman tiene superioridad. Pero es claro que un régimen que no puede verificarse no es creíble. Nuevamente la cuestión de la atribución hace imposible la existencia de un régimen internacional creíble.

En los Estados Unidos siempre existió la idea de que para Rusia era un ejercicio de propaganda. Estados Unidos por su parte no había desarrollado una doctrina y una estrategia sobre la guerra en el ciberespacio, no sabia que hacer con sus desarrollos en las tecnologías de la información y las comunicaciones.

El cambio a la administración Obama modificó la postura de los Estados Unidos que reconoció la peligrosidad de los desarrollos sin control que podrían llevar a una guerra por accidente. Por experiencias anteriores exitosas las tres superpotencias aceptaron la idea de de contar con un foro de comunicación, capitalizando la experiencia en medidas de generación de confianza de otras experiencias de desarme.

El derecho internacional

La aplicación del Derecho Internacional tradicional, del Derecho de la Guerra y del Derecho Humanitario, a las acciones en el ciberespacio que pudieran ser equiparados con un ataque armado ha sido sumamente polémica, y centró las discusiones del Grupo de Expertos.

En su Art. 51, la Carta de la ONU habla del derecho a la legítima defensa "en caso de ataque armado" la discrecionalidad en la aplicación del Derecho a la Legítima Defensa puede ser fuente de inestabilidad y así lo manifestaron en reiteradas oportunidades China y Rusia . Hasta tanto un incidente arriba para su tratamiento al Consejo de Seguridad el estado agraviado se considera con derecho a responder. Tanto EEUU como Rusia han manifestado su disposición a una respuesta cinética, Rusia incluso, con armas nucleares. El principio de la Proporcionalidad en la respuesta a un ataque es difícil de mensurar porque no hay definición de ataque.

Los principios de Distinción entre blancos civiles y militares son imposibles de aplicar en la hipótesis de guerra cibernética ya que no se los puede "marcar". Los actores no estatales tienen más poder en el ciberespacio. Las armas cibernéticas tienen atributos no previstos en las convenciones. Los ejércitos tienen ventajas en mantener sus capacidades secretas. Un ataque cibernético puede incluso no detectarse.

Los Estados tienen derecho a desarrollar armas cibernéticas pero no hay un entendimiento sobre lo que significa

un comportamiento aceptable. La idea de que el Derecho Internacional es aplicable es en realidad un slogan, porque no sabemos cómo se aplicaría. No sabemos qué entender como un acto de guerra, no hay acuerdo sobre la importancia de los incidentes que ocurren, y la mayoría de las discusiones son basadas en especulaciones. ¿Cómo construir un derecho internacional sin casuística?. El trabajo que Rusia y Estados Unidos realizan en el East-West Institute es una indicación clara de las dificultades del tema. (12)

Daño colateral

El principio de distinción indica que sólo está permitido atacar infraestructura militar -no hay que atacar la infraestructura civil. ¿Cómo evitar daños colaterales cuando resulta imposible distinguir un edificio civil de uno militar? ¿Cómo diferenciar una fábrica de aplicaciones militares y un barrio civil? La neutralidad es difícil de establecer porque un atacante puede usar las redes de un país neutral, y por la presencia de proxies. (programa o dispositivo que realiza una acción en representación de otro).

La responsabilidad de los Estados

La asignación de responsabilidad a los Estados por ataques cibernéticos, tema vinculado directamente al de la atribución, presenta varios niveles de análisis:

En un primer nivel, los Estados son responsables por las acciones que cometen intencionalmente a través de sus funcionarios, agentes u organismos o a través de terceros que operan "por cuenta "de este Estado. A este respecto no hay dudas, aunque existieran todas las dificultades en relación la atribución del hecho, pero probado el hecho la responsabilidad del Estado que perpetró el ataque esta fuera de cuestión.

En segundo lugar, los Estados en ejercicio de su poder soberano tienen el derecho y la obligación de asegurar en su territorio el cumplimiento de sus propias leyes y de la ley internacional en relación a la conducta de los habitantes sometidos a su jurisdicción.

Por lo tanto, si aún sin la intención ni consentimiento de las autoridades de un Estado, habitantes o grupos particulares, llevan adelante un ataque cibernético contra otro Estado, podría asignarse responsabilidad al primero si se prueba la negligencia, inacción o falta de cooperación del Estado desde el cual partieron los ataques.

Una tercera posibilidad se presenta en el marco del fenómeno digital cuando se produce un incidente o ataque cibernético en el cual un Estado (A) es "usado" por medio de sus redes como "transito" para un ataque que golpea a un tercer Estado (B). En este caso el Estado A que sirvió de transito, no ha originado el ataque, ni sus autoridades ni sus habitantes han tenido participación alguna, sino que el ataque se ha originado en otro Estado (C). En este caso, hay algunas opiniones que sostienen la posibilidad de asignar responsabilidad al Estado A por no disponer de una vigilancia de sus redes que hubiera permitido bloquear el ataque. Este sería un caso asimilable a la responsabilidad objetiva. Se complica aún más con la Doctrina (Bush) de la Guerra Preventiva. Estados Unidos invade Irak "por las dudas" por la supuesta presencia de al-Qaeda responsable del 11 de Septiembre y la supuesta tenencia de armas de destrucción masiva, adjudicación de responsabilidad que se demostró falsa.

Que los Estados asuman responsabilidad por lo que ocurre en su territorio tiene sentido en el mundo físico en el que la soberanía es un concepto territorial. En el mundo virtual, es más complicado por las dificultades de identificar al agente responsable por la acción. Primero, es difícil para un Estado controlar todo lo que ocurre en su ciber espacio y segundo, más complicado aún es controlar que un tercero no esté usando sus redes para lanzar un ataque.

Por las características de los ataques y las dificultades de atribución, un estado podría terminar invadiendo a quien se le de la gana. El ciber espacio, por sus características de vaguedad e imprecisión genera muchas más oportunidades para el uso discrecional de la fuerza como represalia justificada en el derecho a la legítima defensa de la Carta. La vaguedad hace todo muy peligroso porque somete a los Estados a la discrecionalidad de los más poderosos...

Los estados pueden asumir la responsabilidad por los incidentes cibernéticos que aparecen como originarios de su territorio siempre y cuando cuenten con un nivel de cooperación que les permita ejercen la soberanía en su espacio virtual. Sería más efectivo que los países desarrollados ayuden a los países a conseguir una estructura que permita ocuparse del crimen que convencerlos a que firmen la Convención de Budapest contra el Ciber Crimen; aunque asumir los compromisos de la Convención puede también abrir el camino de concientización doméstica de la necesidad de ocuparse del problema y tener una estructura institucional montada y funcionando.

La cuestión de la libertad de información y los derechos humanos

Ya vimos que los asiáticos consideran a la información como un arma en si misma que puede ser usada para desestabilizar políticamente. Esta fue una de las cuestiones más discutida en las reuniones del Grupo de Expertos Gubernamentales. Tiene sentido, ya que el antagonismo refleja, de alguna forma, los valores de las sociedades liberales de occidente y las no liberales de Asia, pero también revela las cicatrices de la experiencia histórica de los países que han sufrido la desestabilización mediante el uso de la información.

Estados Unidos y las democracias occidentales presionan a favor de un ciberespacio libre de interferencias políticas en el cual la libertad de expresión y de información esté garantizada. Sin embargo, sin hacer consideraciones sobre la buena fe del argumento occidental, una posición muy absoluta no puede triunfar porque con la excusa de la seguridad nacional, la protección a la propiedad intelectual, la armonía social, etc., los propios países occidentales limitan esa libertad. Como resultado, hay que se bastante laxo en la interpretación y aplicación de este principio. (13)

Desde una perspectiva de la paz y seguridad hay que subrayar la importancia que tiene para los Estados conocer la percepción de las amenazas que tienen todos los países para poder actuar en consecuencia. No se debiera intentar cambiar la forma de pensar de los rusos ni de los chinos sino conocer cuáles son sus preocupaciones de ciber seguridad. Me parece que con la información sobre el NSA esta discusión está perdida para Occidente.

Relaciones con el sector privado

Internet es un "common", pero parcelado; es propiedad de y operado por múltiples actores privados. Tal como está estructurado hasta hoy el fenómeno digital, el rol del sector privado es central. Son los dueños de la infraestructura, de

las aplicaciones, son proveedores de servicios, desarrollan el software, dan la tecnología para proteger la infraestructura, son la primera línea de defensa de protección de la red y contra su uso incorrecto.

El papel del sector privado afecta a la Gobernabilidad de Internet, intermedia en las políticas de información y comunicación de los Estados. Las empresas globales tienen cuestiones de jurisdicción con los países en donde localizan sucursales y tienen relaciones con los usuarios. Todos estos roles generan cuestiones que deben ser, discutidas, entendidas y atendidas.

La forma en que se organiza la cooperación pública privada cambia con los países de acuerdo a su historia y cultura. El desarrollo del sector de lasTecnologías de la Información y de las Comunicaciones como política pública también marca la forma de la cooperación; por un lado porque muchas empresas crecieron a la sombra de políticas públicas de promoción, y en muchos casos los actores en el sector público y privado se desempeñaron en una u otra oportunidad en ambos lados del mostrador porque el pool de recursos humanos es limitado.

Los Gobiernos tienen diferentes visiones de cómo debe darse la relación. Las empresas nacionales del país sede plantean una situación y otra diferente las empresas globales que responden a demandas jurisdiccionales que se superponen entre sucursales y matriz. Da la impresión de que la cooperación ad-hoc y a nivel técnico ha sido siempre más sencilla, y más dificultosa al nivel político/legal. Institucionalizar estas relaciones con formas aceptadas en el consenso internacional es importante para resolver el intríngulis que las empresas globales presentan cuando tienen oficinas y negocios en países extranjeros. Un consenso internacional sobre el tratamiento más adecuado, legitimaría la acción de los gobiernos, evita una carrera hacia los estándares más bajos en donde los gobiernos más débiles son los más vulnerables, garantiza un mejor clima de confianza indispensable para el desarrollo de Internet.

La literatura sobre la globalización con frecuencia indica que el crecimiento de Internet da poder a los actores no estatales y debilita el poder de los estados en la gobernabilidad global. Esta literatura está equivocada, los estados y en particular los más poderosos siguen siendo los actores primarios en el diseño de los regímenes internacionales. (14)

Los estados más poderosos cuidan la apariencia de que ninguna persona, organización o gobierno aparezca como responsable en forma completa del funcionamiento de Internet. Internet es una gran red conformada por muchas redes independientes interconectadas voluntariamente entre sí. Funciona sin un órgano de gobierno central, su "gobernabilidad" sucede por la coordinación descentralizada e internacional de una red de múltiples partes interesadas que incluye a gobiernos, sociedad civil, el sector privado, las comunidades académicas, la comunidad técnica y organizaciones nacionales e internacionales.

Cada Estado trata de influenciar la Gobernabilidad de Internet en lo mejor de sus habilidades. La ventaja, sin duda la tienen los Estados Unidos por dos razones, en primer lugar por su participación a través del Departamento de Comercio y por otra parte por tener las empresas más poderosas del sector. De ahí su interés en el modelo multiparticipativo: tiene el Departamento de Comercio, las empresas más importantes y los recursos como para armar la sociedad civil con una agenda propia que no necesariamente representa los intereses de la comunidad internacional en general o el bien común. (15)

Otra cuestión central en las relaciones con el sector privado, es la llamada "responsabilidad del intermediario", los países quieren controlar el contenido que circula por las redes ya sea por razones políticas, religiosas, culturales, etc.; por ello los estados intentan hacerlos responsables por el contenido de lo que pasa por su red. (16)

En la cuestión del espionaje un tema central es la relación de las empresas globales con sus casas matrices y la entrega de información sobre los ciudadanos del país en donde están localizadas sin la autorización judicial correspondiente. Es claro que sin la cooperación del sector privado las escuchas no podrían haberse realizado, no sólo las empresas proveen información a las agencias de seguridad sino que además colocan vulnerabilidades en las aplicaciones para que sean hackeadas con mayor facilidad. (17)

Una tercera, se relaciona con la capacidad de las empresas privadas de hacer justicia con mano propia, contraatacando frente a lo que consideran la violación de un derecho. (18)

Si Internet es participativo, las responsabilidades de cada participante deben estar claramente establecidas en los ámbitos nacionales y en el internacional. Me parece que el consenso sobre cuál es el comportamiento aceptable por parte del sector privado al respecto es bueno para todos y asegura que todos los "interesados", incluso el sector privado, haga su aporte a la salud de Internet aunque les pueda resultar en mayores costos. El consenso no puede resolverse con regímenes voluntarios ya que los mismos han demostrado ser totalmente ineficaces en todas las industrias.

La búsqueda de un régimen internacional

Rusia fue el primer país que llamó la atención sobre los nuevos desafíos del ciberespacio. Durante mucho tiempo intentó generar un espacio de discusión de régimen de control del Ciberespacio en forma bilateral con Estados Unidos. Fueron los primeros en poner de relevancia la importancia de la cooperación internacional para conseguir una respuesta política adecuada al uso de las tecnologías de la información y comunicación para cometer delitos, para desestabilizar políticamente, para el terrorismo y para la guerra. (19)

Rusia tiene claramente definida la necesidad de controlar su "Information Space", para mantener su estabilidad política y poder usar la tecnología para mantener su influencia en la periferia que considera parte de su seguridad nacional. Busca escenarios predecibles en los temas de seguridad internacional en el ciberespacio con manejos responsables. Desarrolla capacidades para ser un actor que pueda limitar la acción de otros, a la vez que favorecerse económicamente de los recursos desarrollados en el mercado de la seguridad informática. (20)

Estados Unidos hace más de veinte años que comienzan a incorporar las Tecnologías de la Información a su doctrina militar. En 1995 se graduó la primera promoción de ciber guerreros de la National Defense University. En lo internacional, se focalizó en evitar la regulación en los aspectos comerciales de Internet, mostró preocupación por el control de exportaciones de tecnología hacia los países del este, propiedad intelectual, terrorismo y crimen organizado y apoyó la Convención de Budapest contre el Ciber-Crimen. En lo relativo a guerra, opinó que para eso está el Derecho Internacional.

En la percepción rusa para Estados Unidos las Tecnologías de la información son una herramienta importante para potenciar su poderío militar y les gustaría permanecer libres del control para poder usarlas a discreción en aplicaciones militares y políticas y quedar fuera de las regulaciones del Derecho Internacional.

En las reuniones del grupo de expertos de Naciones Unidas, los Estados Unidos han insistido sólo en los aspectos tecnológicos de proteger las redes del terrorismo y el ciber crimen, y se negaron a discutir "el uso de las redes". (21)

Para la República Popular China, hay dos objetivos fundamentales en el desarrollo de las Tics, modernización económica y control político, objetivos que podrían ser contradictorios si no fueran usados en forma apropiada. Pero aprendieron de Singapur (22). Cuando uno está en China tiene la impresión de que Internet esta viva y es libre. Internet es un gran multiplicador a través del amplio espectro de actividades del estado. Los chinos quieren controlar la información pero tienen una visión más amplia que Rusia. China tiene clara la importancia de participar en los regímenes que definen los estándares técnicos de Internet como Internet Engineering Task Force (IETF) y W3C consorcio que hace normas de aplicaciones para Internet. Otro objetivo es transformarse en un actor dominante en telefonía Mobil. (23)

El liderazgo chino desarrolla el concepto de "guerra asimétrica" que cambió la doctrina militar que el Presidente Mao le explicó a Kissinger y éste relata en su libro "On China" (24). El Presidente Mao hablaba de "overwhelming numbers" pero después de Desert Storm, -que muestra por primera vez el poderío militar estadounidense desde Viet-Nam- se dan cuenta que ese poderío podría aniquilarlos sin perjuicio del número de efectivos que vayan apareciendo. Irak usaba armamento chino cosa que el Gen. Liu Huaqing registró con preocupación porque fue poco efectivo frente a una fuerza superior.

La formación de recursos humanos es fundamental. En 2006 dos universidades chinas contribuyeron con más estudiantes de doctorado a las universidades americanas que ningún otro país, incluido Estados Unidos.

China introduce en el concepto de "informatization" el uso de las tics para una guerra asimétrica. Esta guerra es considerada como "as a true people´s war". El PLA desarrolla capacidades para atacar satélites e inhabilitar Networks como los Scada (Supervisory Control and Data Adquisition) que son los que controlan las centrales de energía o gasoductos (25). Frente a la negativa estadounidense, en 1998 Rusia elige el camino multilateral para introducir el tema. En una carta al Secretario General de las Naciones Unidas, el canciller Ruso le presenta un proyecto de resolución en el que propone un "Inventario de tecnologías para prevenir aplicaciones militares que pudieran compararse con armas de destrucción masiva".

En el año 2004 se forma el primer Grupo de Expertos, en el seno de la Primera Comisión de Desarme que se limitaba a mostrar las disidencias entre Occidente y el resto del mundo. Recién en 2009, con el cambio de administración, Estados Unidos vota favorablemente la Res.64/25 que se aprobó por consenso. En el grupo de 2012-2013 participa Argentina.

El grupo de expertos gubernamentales

El Grupo se reunió con mandato de la Resolución 66/24 adoptado por la Asamblea General el 2 de Diciembre de 2011. Se solicitaba al Secretario General en el párrafo 4 de la Resolución convocar un Grupo que "continúe el estudio de las amenazas potenciales en el área de la seguridad de la información y posibles medidas de cooperación para ocuparse de ellos, incluyendo normas, reglas o principios de comportamiento responsable de los Estados y medidas de generación de confianza relativas al espacio informativo".

El Secretario General nombró un Grupo compuesto por quince expertos nombrados por los Gobiernos de Argentina, Australia, Bielorusia, Canadá, China, Egipto, Estonia, Francia, Alemania, India, Indonesia, Japón, la Federación Rusa, Reino Unido y los Estados Unidos.

El Grupo se reunió en tres ocasiones durante una semana cada vez: en Agosto del 2012 en Naciones Unidas en Nueva York, en Enero 2013 en Ginebra y en Junio del 2013 nuevamente en las oficinas centrales de las Naciones Unidas en Nueva York.

Como lo solicitara la Resolución, el Grupo tomó como punto de partida el Informe del Grupo anterior que fuera liderado por Rusia.

Durante las reuniones el Grupo discutió las amenazas, los riesgos y las vulnerabilidades de las tecnologías de la información; las formas y medios de cooperación para lograr un ciber ambiente seguro, abierto y flexible; acordaron recomendaciones sobre normas y reglas y principios de comportamiento responsable por parte de los Estados; y las medidas de generación de confianza, intercambio de información y las medidas destinadas a mejorar las capacidades de los Estados. Se logró un informe por consenso.

Las tecnologías de la Información son de uso dual y se pueden usar para usos legítimos o maliciosos. Las amenazas a los individuos, empresas, e infraestructuras nacionales han aumentado y los incidentes son más dañinos. Las amenazas provienen de actores estatales y no estatales, de individuos y grupos que pueden actuar como proxies de Estados en llevar adelante acciones ciber maliciosas. La ausencia de un entendimiento común con relación al uso de las tecnologías de la información aumenta el riesgo a la paz y seguridad internacionales.

El aumento del uso de las tecnologías en las infraestructuras críticas y sistemas de control industrial generan nuevas oportunidades de incidentes. El crecimiento del uso de las tecnologías móviles, redes sociales y el servicio de la nube aumenta los desafíos a la seguridad. Las diferencias en las legislaciones nacionales aumentan las vulnerabilidades, lo mismo los diferentes niveles de capacidades entre Estados.

Los Estados Miembros del Grupo afirmaron en forma reiterada la necesidad de acciones cooperativas contra las amenazas resultantes del un uso malicioso de las tecnologías de la información.

Con relación a las normas, reglas y principios de comportamiento responsable, la aplicación de las normas derivadas del derecho internacional tradicional son de utilidad.

Esencial para reducir riesgos. Entendimientos comunes sobre cómo aplicarlas requiere estudios adicionales. Dada la naturaleza de la tecnología es probable que normas adicionales deban ser desarrolladas. El Derecho Internacional, en particular la Carta de las Naciones Unidas es aplicable y es esencial para mantener la paz y la estabilidad y promover un ciber ambiente abierto, pacífico y seguro.

Los Estados son soberanos y las normas y principios internacionales que emergen de la soberanía son aplicables a la conducta de los Estados en relación al uso de las tecnologías de la información y la jurisdicción sobre la infraestructura en su territorio. El esfuerzo de los Estados por un uso seguro de las tecnologías debe ir acompañado por el respeto a los derechos humanos y las libertades fundamentales. Los Estados deben intensificar la cooperación contra el crimen organizado y el terrorismo. Los Estados son responsables por sus actos, no deben usar proxies para cometer actos impropios y deberían asegurar que sus territorios no son usados por actores no-estatales para un uso ilegal de las Tecnologías de la Información.

El Informe indica una serie de medidas para generar confianza entre los Estados y reducir los riesgos de conflicto incrementar la predictibilidad y reducir las probabilidades de percepciones equivocadas. Alentar el intercambio de información sobre las estrategias nacionales, políticas, mejores prácticas, procesos de decisión y organizaciones nacionales relevantes. Crear marcos consultivos, bilaterales, regionales y multilaterales; mejorar el nivel de intercambio de información entre los Estados sobre los incidentes ocurridos. Intercambio de Información entre CERTS (Computer Emergency Response Teams) ya sea en forma bilateral o multilateral; aumentar la cooperación para ocuparse de los incidentes que puedan afectar la infraestructura crítica de los países y mejorar los mecanismos de cooperación entre los organismos encargados del poder de policía.

El Informe dio mucha importancia a la cooperación internacional en materia de desarrollo de capacidades para que todos los Estados estén en condiciones de ser responsables. A veces es la infraestructura crítica, en otros casos el desarrollo de recursos humanos, o esfuerzos legislativos y relativos al marco regulatorio que les permita cumplir con sus responsabilidades.

El diferente papel de los “interesados” en la seguridad y en un uso apropiado de las tecnologías de la información es de especial relevancia para el Grupo ya que Estados, empresas y sociedad civil tienen responsabilidades compartidas en la seguridad del ciber espacio.

Algunas especulaciones y preguntas

El ciber espacio ofrece nuevos y complicados desafíos para los Estados, los individuos y la sociedad. Desde la perspectiva de las Relaciones Internacionales se parte de una enorme precariedad conceptual y resulta difícil visualizar el futuro sobre un presente que se mueve a gran velocidad.

Es importante subrayar que el ciber espacio sigue siendo un dominio humano y los valores de cada sociedad se reflejarán en el uso que haga de las tecnologías de la información. Como dominio humano, el conflicto en el ciber espacio no altera la naturaleza del conflicto tradicional. Sin embargo, desde una perspectiva de la seguridad internacional hay cuestiones importantes a considerar.

1. La administración del conflicto en el Ciberespacio muestra dificultades por su estructura institucional. El sistema multiparticipativo es intrínsecamente inestable y genera dificultades importantes para las relaciones internacionales que no hay que obviar. El modelo Westfaliano es un sistema de relacionamiento entre los Estados que es territorial, predecible con actores conocidos, mientras que el modelo de Internet es virtual, en apariencia más plano, con un gran poder de generación de impredecibles sinergias entre Estados, y un sinnúmero de actores desconocidos: empresarios, sociedad civil, activistas, crimen organizado, etc. Los efectos de dichas sinergias son difíciles de predecir y sus eventuales consecuencias para la seguridad internacional podrían tenernos especulando por mucho tiempo.
2. La precariedad conceptual sobre lo que se considera un ataque, las dificultades en su atribución, un incipiente desarrollo en una teoría de la disuasión propia del dominio. Las dificultades del control, la asimetría que genera la paradoja de las capacidades y las dificultades de aplicar el Derecho Internacional de la Guerra y del Derecho Humanitario generan situaciones de incertidumbre e inestabilidad.
3. Con relación a la guerra: hay quienes entienden que es un peligro real e inminente (26), otros que se dará en el contexto de un conflicto tradicional, y un tercer grupo cree que el peligro está muy exagerado. (27)

   Personalmente, me inclino por pensar que la Guerra cibernética, se dará en el contexto de un conflicto armado; ahora bien, es claro que existe un peligro potencial cuyo capacidad de desestabilizar se desconoce y que debe ser estudiado en profundidad. Sin perjuicio de evitar las tentaciones del complejo-industrial-cibernético que agudiza la percepción de las amenazas a efectos de favorecer un clima de aumento de inversión en ciber seguridad. (28)
4. Una relación acordada de los Estados con el sector privado y la sociedad civil es de fundamental importancia para la estabilidad del sistema internacional y una efectiva lucha contra el crimen en el ciber espacio. La responsabilidad de cada participante de esta estructura multiparticipativa es esencial si queremos darle la mayor predictibilidad posible al espacio cibernético, en ese sentido hay un interés común de todos los participantes que están a favor de un Internet seguro y sano de cooperar en este sentido. A las vulnerabilidades de la red debiera oponerse la actitud cooperativa de quienes comparten la idea de una red que contribuya al desarrollo y estabilidad de los pueblos.

   Quizás la consecuencia más grave del espionaje haya sido el debilitamiento deliberado de la seguridad de la redes para facilitar la tarea de los Servicios de Inteligencia que, paradojalmente, fue el centro de la doctrina de los Estados Unidos sobre seguridad en el ciberespacio.
5. En cuestiones como la Gobernabilidad, hay que tener presente, que a medida que la brecha digital se achica cambian los protagonistas de este mundo virtual. Internet, que empezó como una cultura libertaria, se mueve hacia una estructura social diferente. Los nuevos actores tienen aspiraciones, intereses y valores muy diferentes que deberán ser tomados en cuenta; es probable que pasemos de una “moralidad” occidental y desarrollada, a otra diferente provenien-

te de sectores que sufren mayores privaciones, más subdesarrollada en donde la ventaja de la asimetría tenderá a aplanar las realidades virtuales y jugar a favor de los más débiles. Lo que es delito en una sociedad significa oportunidad de salir de la miseria en otra. La imagen de un Internet cromado y brillante es desplazada por la realidad de las villas miseria del mundo. De los 55 países con mayor penetración de Internet (2008-2009) 18 son los más pobres y menos desarrollados del planeta, su influencia en Internet será creciente al margen de las preferencias de los grandes actores. (29)

7. En la cuestión de Derechos Humanos, Hay una tensión inherente entre "seguridad-libertad". Los Estados tratarán de vigilar las conductas de sus ciudadanos, con tendencias al estado policial en sociedades sin tradición democrática, pero también con fuertes fuerzas anti-liberales en países con una tradición democrática débil y aún en los occidentales. También emergen tensiones opuestas entre "gran hermano-pequeño hermano" "surveillance vs. susveillance": la misma tecnología que hace posible la emergencia del gran hermano posibilita la emergencia del ciudadano común que por casualidad se encuentra en posición de ser testigo de acontecimientos de gran importancia pública y comparte la información. Les da transparencia: el panóptico al revés. (30)

8. En la planificación para la Defensa, para países como la República Argentina existe la gran tentación de compensar las debilidades de un ejército pequeño con un gran desarrollo para la guerra cibernética. Esto sería un error, necesitamos todos los recursos de las tecnologías de la información y la comunicación para el desarrollo. Por otra parte es un dominio de claro control civil: nuestras Fuerzas Armadas no son red céntricas y nuestra infraestructura crítica es civil.

9. Para una tecnología que supuestamente ignora las fronteras y une al mundo, Internet sufre en la actualidad de una retórica nacionalista muy fuerte (31). Si la palabra clave para un Internet productivo es la confianza, estamos en las antípodas; se puede apreciar preocupación por el origen de los productos de tecnología de la información y servicios, por la cadena de valor de los productos provenientes de China; los países europeos desconfían del servicio de la nube ofrecido por las empresas de los Estados Unidos; nadie sabe si el software y el hardware proveniente de empresas israelíes son confiables en relación del respeto a la privacidad. La Federación Rusa desarrolla sus recursos humanos propios y construye su propio sistema operativo. La República Popular construyó una nueva "gran muralla". Los Ministerios de Relaciones Exteriores de muchos países consideran volver al sistema de comunicaciones encriptadas a la vieja usanza de la Segunda Guerra Mundial.

10. Frente a este escenario, es lógico que los estados quieran mayor control sobre la Internet dentro de sus fronteras, este movimiento de soberanía se reflejó en la reunión de la Unión Internacional de Telecomunicaciones en Dubai (32) y tendrá impacto sobre el esquema multiparticipativo de gobernabilidad.

11. Siempre entendí que si bien la política manda, las soluciones políticas dependen de encontrar una solución técnica que la permita. Aún si nos sentimos agraviados por el espionaje, lo que podamos hacer al respecto esta condicionado por la tecnología. Podemos hablar de responder al agravio con un "Internet nacional", pero la reducción de la brecha digital, la necesidad de conectarnos en algún momento con el resto del mundo, las capacidades técnicas propias y las ajenas, puede dejar nuestra respuesta a nivel de retórica para consumo doméstico.

Claro que a la velocidad que avanza la tecnología todo lo que escribí puede ser historia vieja en muy poco tiempo.

Notas

(1) En muy poco tiempo pasó de ser herramienta de investigación a algo que cubre todo. La infraestructura de Internet pasó a ser Infraestructura crítica y es preocupación prioritaria de los gobiernos protegerla. Ronald Deibert y Rafal Rohozinski "Contesting Cyberspace and the Coming Crisis of Authority" en "Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace" Cambridge MA. MIT Press. 2010

(2) J. Carr "Inside Cyber Warfare" "Mapping the Cyber Underworld"

(3) Kello, Lucas. "The Skeptics Misconstrue the Cyber Revolution: A Response to Commentators on ISSF/H-Diplo and Elsewhere," H-Diplo/ISSF (October 28, 2013)

(4) Ronald Deibert y Rafal Rohozinsky consideran el delito como un "Vector oscuro" del conflicto en el ciber espacio. "Contesting Cyberspace and the Coming Crisis of Authority". En "The Shaping of Power, Rigths, and Rule in Cyberspace" MIT Press 2010

(5) "Cyber War" Richard A. Clarke and Robert Knaye. Harper Collins. 2010

(6) Para un análisis detallado:"Untangling Attribution", David Clark & Susan Landau, Harvard National Security Journal Vol.2/ 2011

(7) Clarke

(8) "Panetta Spells Out Roles in Cyberdefense" (American Forces Press Service Washington DC Oct.11 2012)

(9) Some of this actions have reached too far and we´re going to try to make sure it doesn´t happen in the future" The Guardian 1 de Noviembre de 2013

(10) En el mismo sentido Kristoff en La Nación del Sábado 1 de Nov. 2013

(11) Cuadro desarrollado por Clarke en pag.148

(12) Working Towarsds Rules for Governing Cyber Conflict, Rendering the Geneva and Hague Conventions in Cyberspace by Karl Frederick Rauscher & Andrey Korotkov January 2011

(13) esta fue una de las conclusiones del panel sobre Ciber normas del Workshop - Harvard, MIT, University of Toronto- mayo del 2012)

(14) Drezner cap. 4 pag 117

(15) "Even when States agree about regulatory outcomes, great Powers will will delegate regime Management to non state actors, where their influence still dominates the outcome" Daniel W. Drezner All Politics is Global, Explaining International Regulatory Regimes" Ch. 4 Global Governance of the Internet" Princeton University Press 2007

(16) Ethan Zuckerman "Intermediary Censorship"

(17) Alan Ruisbridger "The Snowden Leaks and The Public"Como las revelaciones de Snowden mostraron, se hizo obvio cuanto dependen los servicios secretos de las firmas comerciales que todos usamos: proveedoras de servicios de Internet, teléfonos, redes sociales.. NYRB Nov.21,2013 issue

(18) Joseph Menn: Hacked companies fight back with controversial steps. Reuters Junio 18 2012.
(19) International Information Security, Problems and Decisions autores varios, compilación de expertos rusos Moscow 2011 Edited by Komov S,A.
(20) Mas info en Carr pag. 217
(21) IIS Problems and Decisions
(22) Daniel Drezner "Global Governance of the Internet" pag.97
(23) "Chinese White Paper on Internet Policy" mimeo
(24) Kissinger, Henry "On China" Penguin Press New York 2011
(25) Inside Cyber Warfare Jeffrey Carr pag.171- también Harvard, MIT "Cyber Norms Worshop" 2012- Panel 2 Challenges to Western Governance"
(26) Kello, Lucas "The Meaning of the Cyber Revolution, Perils to Theory and Statecraft. International Security", Vol. 38, N2 (Fall 2013)
(27) Gartzke, Erik "The Myth of Cyberwar, Bringing War in the Cyberspace Back Down to Earth" International Security, Vol.38, N2 pp.41-73
(28) "Hacking incidents and the rise of the new Chinese bogeyman" Haroon Meer en ALJAZEERA 25 FEB. 2013
(29) Deibert, Ronald and Rohozinski, Rafal "Contesting Cyberspace and the Coming Crisis of Authority" en "Access Controlled: The shaping of Power, Rights, and Rule in Cyberspace" Ed.Deibert,Palfrey, Rohozinskiy Zittrain. MIT Press 2010 pp21-35
(30) "Little Brother Is Watching You, Privacy in the Era of Leaked Recordings" Maria Bustillos The New Yorker, May 22 2013
(31) Schneider, Bruce "Online Nationalism" MIT Technology Review March 11 2013
(32) Tim Wu habla de la persistencia de lo físico en Internet. "La amenaza del uso de la fuerza por parte de los Estados, a través de la ley, dará forma a la red tanto como lo hicieron las ambiciones de sus fundadores. "The Next Digital Decade: Essays on the Future of Internet" Edited by Berin Szoka $ Adam Marcus- TechFreedom.org

Naciones Unidas A/68/98*

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.

13-37169* (S) 050813 070813

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

Prólogo del Secretario General

Las tecnologías de la información y las comunicaciones están entretejidas 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 redunda 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 afectaran 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

MARCO NORMATIVO:

Con excepción de las leyes de Firma Digital (25.506) y Delitos Informáticos (26.388), no se han dictado en nuestro país normas específicas que regulen las acciones que se despliegan en el mundo digital.
En actividades como el Comercio Electrónico, cuyo incremento cada año es significativo, son de aplicación las normas comunes: Códigos Civil y de Comercio, ley de Propiedad Intelectual (11723), Defensa del Consumidor (24240), etc.
Existe un debate sobre la conveniencia de dictar normas nuevas y especificas que se apliquen a la cuestión digital o la inclusión de estos aspectos novedosos en la normativa existente.

En relación a la Ley de Delitos Informáticos (modificatoria del Código Penal), el criterio legislativo que se siguió fue, acertadamente, no crear una ley con nuevos tipos penales, sino la incorporación de las nuevas figuras de delitos informáticos a los tipos penales ya existentes.
El modelo aplicado, en cierta forma, se inspiró en la Convención de Budapest sobre Ciberdelito del Consejo de Europa, quedando sancionadas todas las conductas delictivas que la Convención prevé. Esto puso al país, desde el punto de vista de su legislación penal de fondo, en condiciones de acceder a la mencionada convención, proceso que ya ha iniciado.

Un aspecto especial vinculado a la seguridad cibernética, es el referido a las infraestructuras criticas.
Mediante la resolución 580/2011 de la Jefatura de Gabinete de Ministros, se creo, en el ámbito de la Oficina de Tecnologías de Información (ONTI) el "Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad"- ICIC.
Este programa tiene como objetivo central la "elaboración de un marco regulatorio específico que propicie la identificación y protección de infraestructuras criticas y estratégicas de las entidades definidas en el Art. 8 de la ley 24.156"
El ICIC se apoya en cuatro grupos de trabajo:

1) **GICI: su principal incumbencia se encuentra en el relevamiento, identificación, y clasificación de las Infraestructuras Estratégicas y Críticas de la Información. Define estas infraestructuras de la siguiente forma: Las instalaciones, redes, servicios y equipos físicos y de TI, cuyo funcionamiento es indispensable para brindar servicios a los ciudadanos y a las instituciones.**
2) **GAP: Es el grupo de trabajo responsable de monitorear los sistemas y servicios informáticos expuestos en las redes. Realiza evaluaciones y calificaciones de Data Centers, mediante auditorias de seguridad en los mismos. Presentará un informe anual sobre la situación en materia de ciberseguridad.**
3) **CERT: Es el equipo de respuesta ante los incidentes informáticos, atendiendo específicamente al sector público. Promueve la coordinación entre las unidades de administración de redes informáticas del sector público nacional, actuando en la prevención, detección, manejo y recopilación de información sobre incidentes de seguridad.**

4) **INTERNET SANO: Es un programa de acción destinado a la edicación y a formar conciencia, especialmente entre niños y jóvenes, respecto al uso de las nuevas tecnologías y los riesgos asociadas a este uso.**

Se ha formado adicionalmente, un grupo experto en temas legales, con el fin analizar y formular propuestas en todo lo vinculado al marco normativo en materia de seguridad cibernética. Este grupo, ha redactada la propuesta de creación de dos nuevas figuras penales: Robo de Identidad Digital y Ataques de Denegación de Servicio (DOS).

Significant Cyber Incidents Since 2006

This list is a work in progress that we update as new incidents come to light. If you have suggestions for additions, send them to techpolicy@csis.org. Significance is in the eye of the beholder, but we focus on successful attacks on government agencies, defense and high tech companies, or economic crimes with losses of more than a million dollars.

1. **May 2006.** The Department of State's networks were hacked, and unknown foreign intruders downloaded terabytes of information. If Chinese or Russian spies backed a truck up to the State Department, smashed the glass doors, tied up the guards and spend the night carting off file cabinets it would be an act of war, but when it happens in cyberspace we barely notice.

2. **August 2006.** A senior Air Force Officer stated publicly that, "China has downloaded 10 to 20 terabytes of data from the NIPRNet (the unclassified military network)."

3. **November 2006.** Hackers attempted to penetrate U.S. military War College networks, resulting in a two week shutdown at one institution while infected machines are restored.

4. **December 2006.** NASA was forced to block emails with attachments before shuttle launches out of fear they would be hacked. Business Week reported that the plans for the latest U.S. space launch vehicles were obtained by unknown foreign intruders.

5. **2006.** Chinese hackers were thought to be responsible for shutting down the House of Commons computer system.

6. **April 2007.** The Department of Commerce had to take the Bureau of Industrial Security's networks offline for several months because its networks were hacked by unknown foreign intruders. This Commerce Bureau reviews confidential information on high tech exports.

7. **May 2007.** The National Defense University had to take its email systems offline because of hacks by unknown foreign intruders that left spyware on the system.

8. **May 2007.** Estonian government networks were harassed by a denial of service attack by unknown foreign intruders, most likely at the behest of the Russian government. Some government online services were temporarily disrupted and online banking was halted. These were more like cyber riots than crippling attacks, and the Estonians responded very well; however, they created a wave of fear in cyber dependent countries like the U.S.

9. **June 2007.** The Secretary of Defense's unclassified email account was hacked by unknown foreign intruders as part of a larger series of attacks to access and exploit DOD networks.

10. **August 2007.** The British Security Service, the French Prime Minister's Office and the Office of German Chancellor Angela Merkel all complained to China about intrusion on their government networks. Merkel even raised the matter with China's President.

11. **September 2007.** Israel disrupted Syrian air defense networks (with some collateral Damage to its own domestic networks) during the bombing of an alleged Syrian nuclear facility.

12. **September 2007.** Francis Delon, Secretary-General of National Defence in France, stated that information systems in France had been infiltrated by groups from China.

13. **September 2007.** Contractors employed by DHS and DOD had their networks hacked as backdoors into agency systems.

14. **September 2007.** British authorities reported that hackers, believed to have come from China's People's Liberation Army, penetrated the network of the Foreign Office and other key departments.

15. **October 2007.** China's Ministry of State Security said that foreign hackers, 42% from Taiwan and 25% from United Sates, had been stealing information from Chinese key areas. In 2006, when China's China Aerospace Science & Industry Corporation (CASIC) Intranet Network was surveyed, spywares were found in the computers of classified departments and corporate leaders.

16. **October 2007.** More than a thousand staffers at Oak Ridge National Labs received an email with an attachment that, when opened, provides unknown outsiders with access to the Lab's databases.

17. **November 2007.** Jonathan Evans, the head of Britain's Security Service (MI5), warned 300 business firms of the increased online threat from Russian and Chinese state organizations saying, "A number of countries continue to devote considerable time and energy trying to steal our sensitive technology on civilian and military projects, and trying to obtain political and economic intelligence at our expense. They...increasingly deploy sophisticated technical attacks, using the internet to penetrate computer networks."

18. **January 2008.** A CIA official said the agency knew of four incidents overseas where hackers were able to disrupt, or threaten to disrupt, the power supply for four foreign cities.

19. **March 2008.** South Korean Officials claimed that China had attempted to hack into Korean Embassy and Korea military networks.

20. **March 2008.** U.S. officials reported that American, European, and Japanese companies were experiencing significant losses of intellectual property and business information to

criminal and industrial espionage in cyberspace. However, details cannot be provided in an unclassified setting.

21. **April – October 2008.** A State Department cable made public by WikiLeaks reported that hackers successfully stole "50 megabytes of email messages and attached documents, as well as a complete list of usernames and passwords from an unspecified (U.S. government) agency." The cable said that at least some of the attacks originated from a Shanghai-based hacker group linked to the People's Liberation Army's Third Department.

22. **May 2008.** The Times of India reported that an Indian official accused China of hacking into government computers. The official stated that the core of the Chinese assault is the scanning and mapping of India's official networks to gain access to content in order to plan how to disable or disrupt networks during a conflict.

23. **June 2008.** The networks of several Congressional offices were hacked by unknown foreign intruders. Some infiltrations involved offices with an interest in human rights in Tibet.

24. **Summer 2008.** The databases of both Republican and Democratic presidential campaigns were hacked and downloaded by unknown foreign intruders.

25. **Summer 2008.** Marathon Oil, ExxonMobil, and ConocoPhillips were hacked and lost data detailing the quantity, value, and location of oil discoveries around the world. One company put the losses in the millions.

26. **August 2008.** Computer networks in Georgia were hacked by unknown foreign intruders, most likely at the behest of the Russian government. Much press attention was given to annoying graffiti on Georgian government websites. There was little or no disruption of services but the hacks did put political pressure on the Georgian government and were coordinated with Russian military actions.

27. **October 2008.** Police discovered a highly sophisticated supply chain attack where credit card readers made in China and used in UK supermarkets had a wireless device inserted in them. The device copies a credit card when it is inserted, stores the data, and transfers the data it has collected once a day via WiFi connection to Lahore, Pakistan. Estimated loss is $50 million or more. The device could be instructed to collect only certain kinds of cards (such as gold cards), or to go dormant to evade detection.

28. **November 2008.** Hackers breached networks at Royal Bank of Scotland's WorldPay, allowing them to clone 100 ATM cards and withdraw over $9 million dollars from machines in 49 cities.

29. **November 2008.** Classified networks at DOD and CENTCOM were hacked by unknown foreign intruders. Even worse, it took several days to dislodge the intruders and re-secure the networks.

30. **December 2008.** Retail giant TJX was hacked. The one hacker captured and convicted (Maksym Yastremskiy) is said to have made $11 million from the hack.

31. **December 2008.** Even tiny CSIS was hacked in December by unknown foreign intruders. They probably assumed that some CSIS staff would go into the new administration and may have thought it might be interesting to read their emails beforehand.

32. **2008.** Britain's MPs were warned about e-mails apparently sent by the European Parliament amid fears that they could be used by Chinese hackers to implant viruses.

33. **January 2009.** Hackers attacked Israel's internet infrastructure during the January 2009 military offensive in the Gaza Strip. The attack, which focused on government websites, was executed by at least 5,000,000 computers. Israeli officials believed the attack was carried out by a criminal organization from the former Soviet Union, and paid for by Hamas or Hezbollah.

34. **January 2009.** Indian Home Ministry officials warned that Pakistani hackers had placed malware on popular music download sites used by Indians in preparation for cyber attacks.

35. **February 2009.** FAA computer systems were hacked. Increased use by FAA of IP-bases' networks also increases the risk of the intentional disruption of commercial air traffic.

36. **February 2009.** 600 computers at India's Ministry of External Affairs were hacked.

37. **February 2009.** French naval aircraft planes were grounded after military databases were infected with the "confickr" virus. Naval officials suspected someone at the Navy had used an infected USB key.

38. **March 2009.** The German government warned that hackers were offering a free version of the new Microsoft operating system that installs Trojans.

39. **March 2009.** Canadian researchers found a computer espionage system that they believe China implanted on the government networks of 103 countries.

40. **March 2009.** Reports in the press say that the plans for Marine Corps 1, the new presidential helicopter, were found on a file-sharing network in Iran.

41. **April 2009.** Wall Street Journal articles laid out the increasing vulnerability of the U.S. power grid to cyber attack also highlighted was the intrusions into F-35 databases by unknown foreign intruders.

42. **April 2009.** Prime Minister Wen Jiabao announced that hacker from Taiwan accessed a Chinese State Council computer containing drafts of his report to the National Peoples Congress.

43. **April 2009.** Chinese hackers reportedly infiltrated South Korea's Finance Ministry via a virus attached to e-mails claiming to be from trusted individuals.

44. **May 2009.** In May 2009, Merrick Bank, a leading issuer of credit cards, claimed it lost $16 million after hackers compromised as many as 40 million credit card accounts.

45. **May 2009.** The Homeland Security Information Network (HSIN) was hacked by unknown intruders. The hackers gained access to the data by getting into the HSIN account of a federal employee or contractor. The bulk of the data obtained was federal, but some state information was also accessed

46. **June 2009.** The John Hopkins University's Applied Physics Laboratory, which does classified research for the Department of Defense and NASA, took its unclassified networks offline after they were penetrated.

47. **June 2009.** German Interior Minister Wolfgang Schaeuble noted, when presenting the Interior Ministry's 2008 security report, that China and Russia were increasing espionage efforts and Internet attacks on German companies.

48. **July 2009.** Cyberattacks against websites in the United States and South Korea, including a number of government websites, were launched by unknown hackers. South Korea accused North Korea of being behind the attacks The denial of service attacks did not severely disrupt services but lasted for a number of days and generated a great deal of media attention.

49. **August 2009.** Albert Gonzalez was indicted on charges that between 2006 and 2008, he and unidentified Russian or Ukrainian colleagues allegedly stole more than 130 million credit and debit cards by hacking into the computer systems of five major companies. This was the largest hacking and identity theft crime in U.S. history.

50. **August 2009.** Ehud Tenenbaum was convicted of stealing $10 million from U.S. banks. Tenenbaum was known for hacking into DOD computers in 1998, which resulted in a sentence of six months of community service from an Israeli court.

51. **November 2009.** Jean-Pascal van Ypersele, the vice-chairman of the United Nations' Intergovernmental Panel on Climate Change, ascribed the hacking and release of thousands of emails, from the University of East Anglia's Climatic Research Unit to Russia as part of a plot to undermine the Copenhagen climate talks.

52. **December 2009.** The Wall Street Journal reported that a major U.S. bank had been is hacked, losing tens of millions of dollars.

53. **December 2009.** Downlinks from U.S military UAV's were hacked by Iraqi insurgents using laptops and $24.99 file sharing software, allowing them to see what the UAV has viewed.

54. **January 2010.** The UK's MI5 Security Service warned that undercover intelligence officers from the People's Liberation Army and the Ministry of Public Security have approached UK businessmen at trade fairs and exhibitions with the offer of "gifts" - cameras and memory sticks - which contain malware that provides the Chinese with remote access to users' computers.

55. **January 2010.** Google announced that a sophisticated attack had penetrated its networks, along with the networks of more than 30 other US companies. The goal of the penetrations, which Google ascribed to China, was to collect technology, gain access to activist Gmail accounts and to Google's Gaea password management system.

56. **January 2010.** Global financial services firm Morgan Stanley experienced a "very sensitive" break-in to its network by the same China-based hackers who attacked Google Inc.'s computers in December 2009, according to leaked e-mails from a cyber-security company working for the bank.

57. **January 2010.** M. K. Narayanan, India's National Security Adviser, said his office and other government departments were attacked by China on December 15. The Prime Minister's office later denied that their computers had been hacked. Narayanan said this was not the first attempt to penetrate Indian government computers.

58. **January 2010.** A group named the "Iranian Cyber Army" disrupted service of the popular Chinese search engine Baidu. Users were redirected to a page showing an Iranian political message. Previously, the "Iranian Cyber Army" had hacked into Twitter in December and with a similar message.

59. **January 2010.** Intel disclosed that it has experienced a cyber attack at about the same time that Google, Adobe and other were attacked. The hackers exploited the vulnerabilities in Internet Explorer software that had been used in the other attacks as well. Intel said that there was no intellectual property or financial loss.

60. **March 2010.** NATO and the EU warned that the number of cyber attacks against their networks had increased significantly over the past 12 months, with Russia and China among the most active adversaries.

61. **March 2010.** Google announced that it had found malware targeted at Vietnamese computer users. Google said that the malware was not especially sophisticated and was used to spy on "potentially tens of thousands of users who downloaded Vietnamese keyboard language software" the malware also launched distributed denial of service attacks against blogs containing political dissent, specifically, opposition to bauxite mining efforts in Vietnam.

62. **March 2010.** Australian authorities said there were more than 200 attempts to hack into the networks of the legal defense team for Rio Tinto executives being tried in China, to gain inside information on the trial defense strategy.

63. **March 2010.** Unknown hackers post the real incomes of Latvian government officials after accessing their tax records, creating political turmoil.

64. **April 2010.** Chinese hackers reportedly broke into classified files at the Indian Defence Ministry and Indian embassies around the world, gaining access to Indian missile and armament systems.

65. **April 2010.** A Chinese telecommunications firm accidently transmitted erroneous routing information for roughly 37,000 networks, causing internet traffic to be misrouted through China. The incident lasted 20 minutes and exposed traffic from more than 8,000 U.S. networks, 8,500 Chinese networks, 1,100 Australian networks and 230 French networks.

66. **May 2010.** A leaked memo form the Canadian Security and Intelligence Service (CSIS) says that "Compromises of computer and combinations networks of the Government of Canada, Canadian universities, private companies and individual customer networks have increased substantially.... In addition to being virtually unattributable, these remotely operated attacks offer a productive, secure and low-risk means to conduct espionage."

67. **July 2010.** A Russian intelligence agent (allegedly named Alexey Karetnikov), was arrested and deported after working for nine months as a software tester at Microsoft.

68. **October 2010.** Stuxnet, a complex piece of malware designed to interfere with Siemens Industrial Control Systems, was discovered in Iran, Indonesia, and elsewhere, leading to speculation that it was a government cyber weapon aimed at the Iranian nuclear program.

69. **October 2010.** The Wall Street Journal reported that hackers using "Zeus" malware, available in cybercrime black markets for about $1200, were able to steal over $12 million from five banks in the US and UK. Zeus uses links in emails to steal account information, which the hackers then use to transfer money into bank accounts they control. 100 "mules", or low end criminals, were arrested for opening bank accounts under false names into which the hackers transferred stolen money.

70. **October 2010.** Australia's Defence Signals Directorate reported a huge increase in cyberattacks on the military. Australia's Defence Minister, john Faulkner, revealed there had been 2400 "electronic security incidents" on Defence networks in 2009 and 5551 incidents between January and August 2010.

71. **December 2010.** British Foreign Minister William Hague reported attacks by a foreign power on the Foreign Ministry, a defence contractor and other "British interests" that evaded defenses by pretending to come from the White House.

72. **December 2010.** India's Central Bureau of Investigation (CBI) website (cbi.nic.in) was hacked and data erased. India blames Pakistani hackers. Sensitive CBI data, stored on computer not easily accessible from the Internet, was unaffected.

73. **January 2011.** Hackers penetrated the European Union's carbon trading market, which allows organizations to buy and sell their carbon emissions quotas, and steal more than $7 million in credits, forcing the market to shut down temporarily.

74. **January 2011.** Hacker extracted $6.7 million from South Africa's Postbank over the New Year's Holiday.

75. **January 2011.** The Canadian government reported a major cyber attack against its agencies, including Defence Research and Development Canada, a research agency for Canada's Department of National Defence. The attack forced the Finance Department and Treasury Board, Canada's main economic agencies, to disconnect from the internet. Canadian sources attribute the attack to China.

76. **March 2011.** Hackers penetrated French government computer networks in search of sensitive information on upcoming G-20 meetings.

77. **March-April 2011.** Between March 2010 and April 2011, the FBI identified twenty incidents in which the online banking credentials of small-to-medium sized U.S. businesses were compromised and used to initiate wire transfers to Chinese economic and trade companies. As of April 2011, the total attempted fraud amounts to approximately $20 million; the actual victim losses are $11 million.

78. **March-April 2011.** Hackers used phishing techniques in attempt to obtain data that would compromise RSA's SecureID authentication technology. The data acquired was then used in an attempt to penetrate Lockheed Martin's networks.

79. **April 2011.** Google reported a phishing effort to compromise hundreds of Gmail passwords for accounts of prominent people, including senior U.S. officials. Google attributes the effort to China.

80. **April 2011.** Employees at Oak ridge National Laboratory received bogus emails with malware attachments. Two machines were infected and "a few megabytes" of data were extracted before the Lab was able to cut its internet connection. Oak Ridge was the target of an intrusion in 2007.

81. **May 2011.** Cybercriminals masquerading as member of the hacktivist group "Anonymous" penetrated the PlayStation network. Sony estimated that personal

information for more than 80 million users was compromised and that the cost of the breach at over $170 million.

82. **June 2011.** The IMF's networks were compromised reportedly by a foreign government using fraudulent emails with malware attachments, and a "large quantity of data, including documents and e-mails," are exfiltrated.

83. **June 2011.** Citibank reported that credit card data for 360,000 of its customers were exfiltrated using a relatively simple manipulation of URLs.

84. **July 2011.** In a speech unveiling the Department of Defense's cyber strategy, the Deputy Secretary of Defense mentioned that a defense contractor was hacked and 24,000 files from the DOD were stolen.

85. **July 2011.** The German Bundespolizei (Federal Police) and the Bundeszollverwaltung (Federal Customs Service) discovered that servers used to locate serious criminals and terrorism suspects by gathering information from GPS systems in cars and mobile phones were penetrated (using a phishing attack)as early as 2010. Following the cyberattack, the relevant servers had to be temporarily shut down to prevent further data losses.

86. **July 2011.** South Korea said hackers from China had penetrated an internet portal and accessed phone numbers, e-mail addresses, names and other data for 35 million Koreans.

87. **August 2011.** According to sources in the Japanese government, Mitsubishi Heavy Industries and twenty other Japanese defense and high tech firms were the target of an effort to extract classified defense information. Japanese officials believed the exploits all originated from the same source. The intruder used email with a malicious attachment whose contents were the same as a legitimate message sent 10 hours earlier.

88. **August 2011.** Email and documents from 480 members of the Japanese Diet and lawmakers and their staff were compromised for a month after a phishing attack implanted a Trojan on members' computers and Diet servers. The hijacked machines communicated with a server in China and the attackers included Chinese characters in their code.

89. **September 2011.** Unknown attackers hacked a Dutch certificate authority, allowing them to issue more than 500 fraudulent certificates for major companies and government agencies. The certificates are used to verify that a website is genuine. By issuing a false certificate, an attacker can pretend to be a secure website, intercept e-mail, or install malicious software. This was the second hack of a certificate authority in 2011.

90. **September 2011.** Australia's Defense Signals Directorate says that defense networks are attacked more than 30 times a day, with the number of attacks increasing by more than 350 percent by 2009.

91. **September 2011.** A computer virus from an unknown source introduced "keylogger" malware onto ground control stations for US Air Force UAVs and, according to press reports, infected both classified and unclassified networks at Creech Air Force Base in Nevada. The US did not lose control of any drone nor does it appear that any data was exfiltrated, but the malware was persistent and took several attempts to remove.

92. **October 2011.** Networks of 48 companies in the chemical, defense and other industries were penetrated for at least six months by a hacker looking for intellectual property. Symantec attributes some of the attacks to computers in Hebei, China.

93. **November 2011.** Norway's National Security Agency (NSM) reports that at least 10 major Norwegian defense and energy companies were hacked. The attacks were specifically "tailored" for each company, using an email phishing scheme. NSM said that the attacks came when the companies, mainly in the oil and gas sectors, have been involved in large-scale contract negotiations. The hacking occurred over the course of 2011, with hackers gaining access to confidential documents, industrial data, usernames and passwords.

94. **December 2011.** U.S. Chamber of Commerce computer networks were completely penetrated for more than a year by hackers who, according to press reports, had ties to the People Liberation Army. The Hackers had access to access to everything in Chamber computers, including member company communications and industry positions on U.S. trade policy.

95. **March 2012.** NASA's Inspector General reported that 13 APT attacks successfully compromised NASA computers in 2011. In one attack, intruders stole 150 user credentials that could be used to gain unauthorized access to NASA systems. Another attack at the Joint Propulsion Laboratory involving China-based IP let the intruders gain full access to key JPL systems and sensitive user accounts.

96. **March 2012.** The BBC reported a "sophisticated cyber-attack" in an effort to disrupt the BBC Persian Language Service. The attack coincided with efforts to jam two BBC satellite feeds to Iran. The BBC's Director General blamed Iran for the incident.

97. **March 2012.** India's Minister for Communications and Information Technology revealed in a written reply to a Parliamentary question that 112 government websites had been compromised from December 2011 to February 2012. Most of the incidents involved website defacement and many of the hacks appeared to originate in Pakistan.

98. **March 2012.** The U.S. Department of Homeland Security issued amber alerts warning of a cyber intrusion campaign on U.S. gas pipelines, dating back to December 2011. Press reports indicated that Industrial Control Systems Cyber Emergency Response

Team (ICS-CERT) described the attack as a sophisticated spear phishing campaign emanating from a single source.

99. **May 2012.** UK officials told the press that there had been a small number of successful perpetrations of classified MOD networks.

100. **May 2012.** An espionage toolkit named "Flame" is discovered in computers in the Iranian Oil Ministry, as well as in other Middle Eastern countries, including Israel, Syria, and Sudan, and other nations around the world.

101. **May 2012.** Researchers at the University of Toronto report that versions of the installer for the proxy tool Simurgh, which anonymizes net use and is popular in countries such as Iran and Syria to circumvent government internet controls, also installs a keylogger Trojan which sends the user name, keystrokes, and program use to another site.

102. **June 2012.** A phishing campaign targets the U.S. aerospace industry experts attending the 2013 IEEE Aerospace Conference.

103. **June 2012.** A global fraud campaign using automated versions of SpyEye and Zeus Trojans targeted high-value personal and corporate accounts and bypassed two-factor authentication.

104. **June 2012.** The head of the UK Security Service stated that a London-listed company lost an estimated £800m ($1.2 billion) as a result of state cyber attacks.

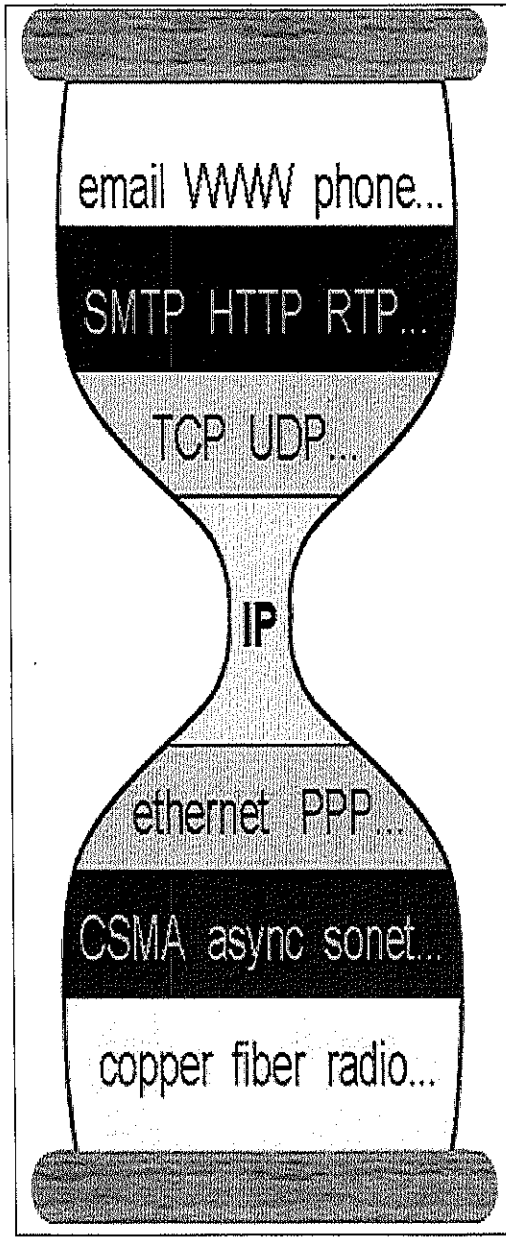
105. **July 2012.** A Trojan nicknamed "Mahdi" found gathering data from approximately 800 critical infrastructure engineering firms, government agencies, financial houses, and academia throughout the Middle East and beyond, predominantly in Israel and Iran. The virus contains Persian language strings.

106. **July 2012.** Indian naval officials confirmed that a virus had collected data from sensitive computer systems at the country's Eastern Naval Command headquarters and sent the data to Chinese IP addresses. The virus allegedly entered the Navy's network via infected USB drives, which were used to transfer data from standalone computers holding sensitive files to networked systems.

107. **July 2012.** The Director of the National Security Agency said that there had been a 17-fold increase in cyber incident at American infrastructure companies between 2009 and 2011.

108. **August 2012.** Malware nicknamed "Gauss," infected 2,500 systems worldwide. Gauss appears to have been aimed at Lebanese banks, and contains code whose encryption has not yet been broken.

El modelo reloj de arena, protocolos, aplicaciones y los actores de la gobernanza de Internet

PROTOCOLOS	APLICACIONES	ACTORES
	Aplicaciones, programas, proveedores de contenido Aplicaciones para móviles Nombres de dominio Aplicaciones de Seguridad Encripción de datos Protección de datos	Google, Youtube,Google maps, etc. Microsoft, Outlook, Skype. Facebook, Netflix, otros proveedores de contenido ICANN (DNS) Proveedores de gestión de contenidos Puntos de Intercambio de tráfico Agencias de seguridad informática, CSIRTS IETF W3C UIT Naciones Unidas
	Numeros de Port Transporte de datos entre redes	Departamento de Comercio de USA IANA, IETF, ISPs Proveedores de Acceso a Internet Administradores de redes y seguridad de redes
	Direcciones IPv4 e IPv6 Enrutadores (routers)	Proveedores de acceso a Internet Grandes empresas de telecomunicaciones Usuarios finales a través de ISPs Grandes redes privadas de datos IETF, IANA, ICANN Departamento de Comercio de USA ICANN (Numeros IP, Servidores Raíz) RIRs: LACNIC, APNIC, RIPE, AFRINIC,
	Redes LAN: redes de área local Redes WAN de área extendida	IEEE UIT IETF
	Cables submarinos de Fibra óptica Redes de tv por cable para acceso cablemodem (como Fibertel) Redes de microondas Redes WiFi, WiMax, Microondas, cables coaxiles, cables de redes de datos.	IEEE UIT Agencias de estándares de la industria eléctrica (cableados, cableado estructurado, antenas) Ministerios y secretarias de comunicaciones, TICs, etc Intel, AMD, fabricantes de equipos electrónicos

IEEE: Instituto de Ingenieros Electronicosy Electricistas – de USA – Desarrollo de estándares de la industria electronica y de comunicaciones

IETF: Internet Engineering Task Force – Desarrollo de protocolos IP

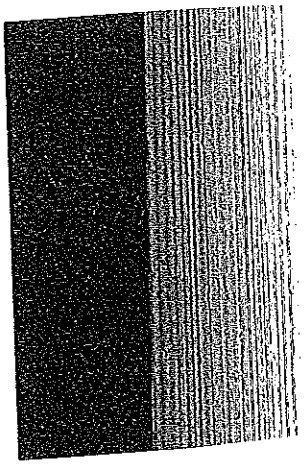
UIT: Unión Internacional de Telecomunicaciones – Ginebra – ONU

ICANN: Corporación de Internet para Nombres y Numeros – USA – coordina el sistema de nombres de dominio DNS y los servidores raíz

IANA: Internet Assigned Numbers Authority – depende del depto de comercio de USA – Es la que tiene la lista general de direcciones IP v4 y v6

RIRS: son los que entregan las direcciones IP al público, empresas, proveedores de Internet, etc. IANA entrega las direcciones a través de los RIRS que son cinco, uno por cada continente. El de nuestra región se llama LACNIC

W3C: consorcio que hace normas de aplicaciones para Internet como accesibilidad por ejemplo, la fundo el inventor del WWW Tim Berns Lee, científico inglés que trabajaba en el CERN en Ginebra y ahora trabaja en el MIT.



OVERALL CYBER WAR STRENGTH

Nation	Cyber Offense	Cyber Dependence	Cyber Defense	Total
U.S.	8	2	1	11
Russia	7	5	4	16
China	5	4	6	15
Iran	4	5	3	12
North Korea	2	9	7	18

Libros

"Born Digital"
Understanding the First Generation of Digital Natives
John Palfrey and Urs Gasser
Basic Books NY 2008

"The Future of the Internet - And How to Stop It"
Jonathan Zittrain
Yale University Press 2008

"The International Legal Instruments and Documents on International Information Security".
Adjemov A.S., Boyko S.M., Dylevsky I.N., Efimushkin V.A., Fedorov A.V., Klimashin N.V., Komov S.A., Korotkov S.V, Krutskikh A.V., Miroshnikov B.N, Petrunin A.N., Polyakova T.A., Sherstyuk V.P., Streltsov A.A., Zaytsev N.L.
Komov S.A. 2012

"Ghost in the Wires"
My adventures as the world's most wanted hacker
Kevin Mitnick with William L. Simon
Back Bay Books 2012

"All Politics Global"
Explaining International Regulatory Regimes
Chapter Four - The Global Governance on the Internet
Daniel W. Drezner
Princeton University Press 2007

"Worm"
The First Digital World War
Mark Bowdwn
Atlantic Monthly Press NY 2011

"International Information Security: Problems and Decisions"
Adjemov A.S., Boyko S.M., Dylevsky I.N., Efimushkin V.A., Fedorov A.V., Klimashin N.V., Komov S.A., Korotkov S.V, Krutskikh A.V., Miroshnikov B.N, Petrunin A.N., Polyakova T.A., Sherstyuk V.P., Streltsov A.A., Zaytsev N.L.
Komov S.A. 2011

"Cyberpower and National Security"
Edited by Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz
Center for Technology and National Security Policy – National Defense University Press – Potomac Books, Inc. Washington DC 2011

"Cyber Warfare"
Techniques, Tactics and Tools for Security Practitioners
Jason Andress
Steve Winterfeld
Elsevier 2011

"The New Digital Age"
Reshaping the Future of People, Nations and Business
Eric Schmidt and Jared Cohen
Alfred A. Knopf NY 2013

"Criptopunks"
La libertad y el futuro de Internet
Julian Assenge
Marea Editorial 2013

"Cyber Warfare and the Laws of War"
Heather Harrison Dinniss
Cambridge University Press 2012

"The Gutenberg Galaxy"
Marshall Mc Luhan
University Toronto Press 2001

"The Future of Ideas"
Lawrence Lessig
Random House NY 2001

"Underground"
Gripping...the bizarre lives and crimes of an extraordinary group of teenage hackers´
Rolling Stone
Suelette Dreyfus & Julian Assenge
Canongate 2012

"Trust me I'm Lying"
Confessions of a media manipulator
Ryan Holiday
Portfolio / Penguin 2012

"The Master Switch"
The Rise and fall of Information Empires
Tim Wu
Alfred Knopf NY 2010

"Communication Power"
Manuel Castells
Oxford University Press 2009

"Googled: The End of the World As We Know It"
Requin books 2010
Ken Auletta

Cyber War
Richard Clarke and Robert Knake
Harper Collins. 2010

Free Culture The Nature and Future of Creativity
Lawrence Lessig
Penguin Books 2003

Eneken Tikk-Ringas (2012)
Developments in the Field of Information and Telecommunication in the Context of International Security: Work of the UN First Committee 1998-2012, ICT4Peace Publishing Geneva.

MIMEOGRAFÍA

"¿Es la Guerra Cibernética el desafío más relevante de la Defensa Nacional?"
Por Roberto Uzal

"Cybersecurity and Cyberwarfare"
Preliminary Assessment of National and Organization
Center for Strategic and International Studies
James A. Lewis, Katrina Timlin 2011

"A Proposal for an International Convention
To Regulate the Use of
Information Systems in Armed Conflict"
Davis Brown
Volume 47, Number 1, Winter 2006

"Why States Need an International Law for Information Operations"
By Duncan B. Hollis
LCB_11_4_ART7_HOLLIS.DOC 2007

"Cultivating International Cyber Norms"
By Martha Finnemore
Chapter VI – America´s Cyber Future – Security and Prosperity in the Information Age
June 2011

"Ten Rules for Cyber Security"
Eneken Tikk
Article was first published in Survival / vol.53 no. 3 / June-July 2011 / pp. 119-132

"The Customary International Law of Cyberspace"
Gary Brown, Colonel, USAF
Keira Poellet, Major, USAF

Strategic Studies Quarterly – Fall 2012

"A Treaty for Cyberspace"
Rex Hughes
International Affairs 86: 2 (2010) 523-541

"Cyberspace, the New Frontier and the Same Old Multilateralism"
Panayotis A. Yannakogeorgos
Chapter V – Global Norms, American Sponsorship and World Politics

"University of Rhode Island Cybersecurity Symposium Keynote Address"
General Keith Alexander, Director of the National Security Agency and US CYBER COMMAND – April 11, 2011.

NOTE: "Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare"
Jeffrey T. G. Kelsey

ESSAY: "Untangling Attribution"
David D. Clark and Susan Landau
2011 Harvard College
The January 2012 report in our Connected World
(https://www.bcgperspectives.com/content/articles/growth_innovation_connected_world_digital_manifesto/)

"Little Brother Is Watching You"
The New Yorker
Posted by Maria Bustillos
May 22, 2013

Manuel Castells: "La sociabilidad real se da hoy en Internet"
Por Horacio Bilbao