El derecho internacional y la seguridad cibernética.

Grl Div (R) Evergisto de Vergara

Como sucede casi todas las veces, los adelantos tecnológicos y sus consecuencias generan normas del derecho después que han ocurrido. La Guerra Informática, Guerra Digital o Guerra Cibernética no es la excepción. Una de las tendencias persistentes en la relación entre guerra y derecho, es que cuando la sociedad en general se involucra en un nuevo ambiente, el derecho tiene que ponerse al día con la tecnología. Eso no debe sorprender: nadie escribe derecho para algo que no existe. Lo contrario sería algo así como pretender escribir el derecho del mar antes que se inventasen los buques, o que se escribiese el derecho del aire antes que se inventasen los aeroplanos.

Las operaciones cibernéticas entran en la categoría de operaciones de información, que se categorizan como operaciones contra el comando y control, operaciones de inteligencia, operaciones psicológicas y operaciones cibernéticas[1], aclarando que las operaciones cibernéticas también se llevan a cabo en las tres categorías arriba mencionadas de operaciones de información.

El tema surge porque a raíz de los adelantos en información y telecomunicaciones, las sociedades se han hecho cada vez más dependientes de las computadoras y las redes de computadoras, que regulan servicios vitales para ellas usando Internet. Curiosamente, aunque la tecnología busque progreso y bienestar, cuanto más dependa una sociedad de esa tecnología, se

[1] Hay que distinguir las operaciones de información, de las operaciones informáticas, digitales o cibernéticas. Estos tres últimos términos son sinónimos.

hará más vulnerable. Los riesgos estratégicos ya no provienen únicamente de juegos de *hackers* [2] adolescentes, sino de activistas ideológicos, de otros Estados, de delincuentes y de terroristas. Las distancias geográficas y las fronteras son irrelevantes, y un ataque informático puede provenir de las antípodas en cuestión de segundos. El equipamiento y el conocimiento están al alcance de todos, es relativamente barato, y así se puede causar grandes daños a un Estado con capacidad militar convencional muy superior. Además, estas acciones son anónimas, y pueden llevarse a cabo no solo durante una guerra convencional, sino también en épocas de paz. Por estas razones, el tema ya está en consideración en Naciones Unidas.[3]

El uso indebido de las facilidades cibernéticas puede ser dividido en áreas: si se trata de agresiones de otros Estados, si se trata de grupos de individuos de diferentes estados con motivaciones ideológicas, si se trata de grupos económicos que buscan información competitiva, si se trata de terroristas trasnacionales, o si se trata de delincuentes comunes. Sin embargo, es difícil separar tan claramente esta categorización, porque además del anonimato tienen varios denominadores comunes: usan la misma tecnología, no necesariamente están asentados en un solo territorio nacional, y pueden usar facilidades instaladas en otros Estados para llevar a cabo sus acciones.

Este ensayo no trata sobre grupos económicos que busquen información competitiva, ni de delitos comunes informáticos. Trata sobre el derecho internacional referente a agresiones de otros Estados, de organizaciones no gubernamentales trasnacionales y del terrorismo internacional. A esto se denomina guerra cibernética, y se analizará esta frase más adelante. Los actos de una denominada guerra cibernética están acompañados de una intención hostil, y están dirigidos a alterar o destruir la información contenida en la computadora o en la red que se ataca, para incapacitar los sistemas de comando y control, sistemas de comunicaciones, difundir propaganda o causar daños que exceden al daño intrínseco de la computador a o red atacada.

Algunos rudimentos tecnológicos

[2] Del inglés *hack*, hachar. Término utilizado para llamar a una persona con grandes conocimientos en informática y telecomunicaciones y que los utiliza con un determinado objetivo. Este objetivo puede o no ser maligno o ilegal. Hoy tiene una connotación negativa, porque se lo relaciona a tareas ilegales.
[3] Naciones Unidas, Documento A/RES/64/211 del 17 de marzo de 2010, *Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures.*

Los ataques cibernéticos con intención hostil de dañar entornos controlados por computadora son, además de su destrucción física, la corrupción de su hardware (*chipping*)[4] o software, o sobrecargando la demanda de información en forma simultánea para causar que colapse (DoS, denegación de servicio por sus siglas en inglés).

Las herramientas de software más populares diseñadas para interferir o dañar el funcionamiento de otras computadoras y redes son los denominados troyanos, bombas lógicas, virus y gusanos, que pueden ser instalados en otras computadoras mediante *chipping*, *hacking* o simplemente, a través de correos electrónicos. Se los generaliza bajo el nombre de *malware,* o software malicioso.

Un virus es un programa que se replica a sí mismo que normalmente se pega a un programa legítimo de la computadora que es atacado, modificando el programa contagiado y los otros programas de la computadora, así como propagándose hacia otras computadoras.

Un gusano se replica en su totalidad en otras computadoras, pero a diferencia de un virus, no modifica otros programas, sino que captura las direcciones de contactos de la computadora atacada y envía automáticamente mensajes a través el sistema que si son abiertos, causan demoras en la operación y eventuales colapsos.

Los virus y los gusanos pueden ser escondidos en troyanos, un fragmento de código aparentemente inocuo que en realidad encubre a un programa dañino o permite el acceso remoto a la computadora atacada por parte de un usuario externo.

Las bombas de tiempo y las bombas lógicas son una clase de troyanos destinados a ser ejecutados en determinado tiempos o bajo ciertas circunstancias. Algunos programas pueden haber sido saboteados por los mismos creadores sin darse cuenta. Por ejemplo, en 1984 y con la tecnología informática disponible en aquel entonces, la Compañía Adobe Systems Inc, accidentalmente incluyó una "bomba lógica" en una versión de su programa popular de Photoshop. Esta "bomba lógica" del programa causaba que éste dejara de funcionar después de

[4] Acción de introducir chips subrepticiamente en una computadora, para explotar sus debilidades o defectos. Un *chip* es un circuito integrado por muchos transistores, en su interior pueden llegar a existir incluso millones de estos, arreglados entre sí para hacer muchas funciones y su composición sobre todo es de silicio. Existe Chips diseñados para miles de tareas electrónicas.

una fecha en particular y había sido incluido dentro del código para forzar a los que tenían la versión de prueba a comprar la versión final. Sencillamente, los vendedores del programa final se olvidaron de quitarlo. [5] Esas "bombas lógicas" son las que están incluidas en la mayoría de los programas de versión libre, que dejan de funcionar luego de un tiempo. Cuando se compra la versión, lo que hace el vendedor es desactivar esa bomba lógica.

En cuanto a los ataques de denegación de servicio (DoS), el objetivo es inundar a la red que se toma como blanco con requerimientos, para sobrecargarlo y así incapacitarlo. Cuando este ataque DoS se lleva a cabo por un número importante de computadoras, se denomina Denegación de Servicio Distribuida (DDoS por su sigla en inglés). Eso pasó en Estonia en el año 2007, y en el peor ataque cibernético que registra la historia el 27 de marzo de 2013. Aquí, la disputa entre dos empresas *Spamhouse*, que tiene sede en Londres y en Ginebra, y se dedica a crear listas negras de los que envían publicidad no solicitada (o spam) añadió a sus bloqueos a *Cyberbunker*, una firma holandesa que ofrece alojamiento para toda clase de contenidos "excepto" – aseguran – pornografía infantil y terrorismo. La respuesta fue un ataque que puso a *Spamhouse* fuera de combate. Pero eso fue solo el principio. Por la técnica de ataque utilizada, los efectos se propagaron por la infraestructura de Internet, haciendo que el acceso a la Web, entre otras cosas, funcionara muy lentamente. En particular, además de *Spamhouse*, se vio afectado un servicio esencial para la Web, llamado DNS.

Por diversos motivos, los servidores DNS pueden ser objeto de ataques informáticos. El problema es que si la traducción de la dirección URL (*Uniform Resource Locator*, o dirección web) que se tipea en la computadora y que es convertida a números IP por el DNS falla o se demora, Internet o deja de funcionar o se pone demasiado lenta. En corto lapso, un ataque Distribuido de Denegación de Servicio (DDoS) envía simultáneamente millones de solicitudes de página al sitio, que por lo tanto se inunda de tráfico y deja de responder. Para esto se usan computadoras personales infectadas con un tipo de software malicioso llamado *botnet* (sigla en inglés por red de robots). Los *botnets* les entregan control remoto de las PC infectadas a los atacantes. Son una pesadilla para los administradores de sistemas y uno de los negocios más ricos de los delincuentes informáticos, que alquilan el tiempo de estas redes para los DDoS, el

[5] Lawrence T. Greenberg y otros, *Information Warfare and International Law*, National defense University, Institute for National Strategic Studies, ISBN 1-57906-001-3, Washington DC EEUU, Año 1998, P. 61 y 62.

envío de virus y la distribución del *spam.* Una nueva técnica, denominada *reflexión del DNS* aumenta la sobrecarga de las redes y sistemas.[6]

El anonimato en una red se lleva a cabo mediante *spoofing* [7], que en términos de seguridad cibernética hace referencia a técnicas de suplantación de identidad generalmente de usos maliciosos o de investigación. Hay *sopoofing* usando servers de anonimato, de público acceso en Internet. La consigna difundida es que el anonimato no es delito.

La guerra cibernética.

En el umbral de una investigación, se deberían plantear ciertas preguntas que será necesario explorar: en la denominada Guerra Cibernética. Si el consenso general es que en una guerra debería haber violencia y bajas humanas ¿Es correcto llamarlo Guerra Cibernética? ¿A cuáles actividades entre individuos, estados y actores no estatales debemos llamar "guerra"? ¿Qué es un acto de guerra? Si se la llamase guerra, ¿Quiénes son los combatientes, y los no combatientes? ¿Es legítimo usar la fuerza convencional para neutralizarla, aduciendo defensa propia? ¿Es aplicable el *jus in bello* en este ámbito? En la era informática, ¿Cómo se aplican los términos usados en la Carta de Naciones Unidas de "fuerza", "agresión" o "ataque armado?¿Cómo se compatibiliza la responsabilidad nacional y el principio de soberanía territorial con los actos y acciones en el ciberespacio, que no tiene fronteras? ¿Podría equipararse los efectos de un ataque cibernético a los de un arma de destrucción masiva? Las consideraciones a que se aribe, ¿Son validas únicamente para acciones entre Estados, o también pueden aplicarse a actores no estatales? ¿Cuál es la responsabilidad de un Estado sobre los delincuentes informáticos y sobre los terroristas informáticos que operen desde su territorio, o que permitan que sus *servers* sean usados de puente en un ataque informático? ¿Pueden implementase controles internacionales que limiten/vigilen los medios informáticos y de telecomunicaciones de los Estados, al estilo de los controles sobre las armas de destrucción masiva? Estas solo serán algunos interrogantes que habrá que formularse y acordar.

[6] Puede encontrarse una explicación más técnica en http://ws.edu.isoc.org/data/2006/570066312448cfa2c134a4/060515.AfNOG-DNS-DDOS.pdf fecha de consulta 20 Abril 2013.
[7] Del inglés spoof, engañar.

Los desastres eventuales que pueden causar los ataques cibernéticos a un Estado, ya sea en guerra o en paz, han motivado que se los considere como una guerra particular. Así, habría que revisar el concepto de *jus ad bellum* que lo justificaría, y el *jus in bello* para determinar la forma de comportarse en esta guerra.

En principio, *el jus ad bellum* es el derecho que asiste a todo Estado para hacer uso de la fuerza. Para eso se requiere que existan siete aspectos: *causa justa*, es decir que sólo se debe confrontar a un peligro real y cierto; *autoridad competente*: la guerra debe ser declarada por aquéllos que tienen la responsabilidad del orden público; *justicia comparativa*: en el caso que los derechos y valores conculcados justifican matanzas; *recta intención; último recurso*: deben haberse agotado todas las instancias pacíficas; *probabilidad de éxito*: debe evitarse todo recurso irracional a la fuerza, o resistencia sin esperanza; y *proporcionalidad*: el daño a ser infligido y los costos en que se incurran deben ser proporcionados al bien que se espera obtener.

En breve, se considera que es una guerra porque implica un ataque, luego sería legítimo defenderse. Implica también tomar medidas de seguridad previas a cualquier ataque cibernético, pero esa seguridad se refiere no únicamente a las agresiones de otros Estados, sino que también protege contra delincuentes, robo de información estatal, y contra terroristas cibernéticos. No existiría una guerra en el concepto tradicional, si alguien no atacase y otro no defendiese. Además, las consecuencias de un ataque cibernético puede implicar destrucción de infraestructura crítica y ello puede causar pérdida de vidas cuantiosas o catastróficas en la propiedad.

También el ataque cibernético, en principio una agresión no incluida por la ONU en su definición de la UN Res AG 3314/74, puede tomar diferentes formas: un acto aislado en época de paz, una acción previa a un conflicto convencional, el primer golpe de un conflicto convencional, una acción durante el desarrollo de un conflicto convencional, o una represalia en reacción a un conflicto convencional o ataque cibernético.

Para demostrar lo difícil de diseccionar el tema, ya desde el comienzo debe aceptarse que la adquisición de información subrepticia de un Estado sobre otro Estado se denomina espionaje, y el derecho internacional no lo prohíbe, aunque en el derecho interno de los Estados afectados se sanciona. La nueva categoría es *ciberespionaje*, y se lleva a cabo por "puertas

trampa"[8] u "olfateadores"[9]. También las operaciones cibernéticas se usan como vehículo de propaganda: en Agosto de 2008, un ataque cibernético tuvo lugar en Georgia previo a la invasión rusa a Ossetia del Sur, donde el contenido de las páginas web de las Agencias de Información de Georgia fue modificado. La inteligencia rusa fue acusada, pero negó tal cargo aunque su participación era altamente probable.

El concepto de soberanía territorial no se ajusta demasiado al concepto de ciberespacio. Tampoco hay acuerdo internacional si un ataque cibernético puede ser considerado en las mismas condiciones de un ataque armado. Inicialmente, todos están de acuerdo que los poderes nacionales defiendan sus infraestructuras críticas. Los problemas surgen cuando deben clarificar si usarán medidas defensivas, ofensivas o de represalia. Toma renovada vigencia lo dicho por Clausewitz: *La forma defensiva de la guerra no es simplemente un escudo, sino un escudo hecho de golpes bien dirigidos.* [10]

No se ha establecido, está en discusión y hay opiniones diversas sobre si un ataque cibernético, en especial si no tiene fuerza letal o destructiva de bienes materiales, constituye lo que en Naciones Unidas se entiende por "uso de la fuerza" o "ataque armado". Mientras unos sostienen que solo es parte de coerción y por lo tanto no pueden usarse fuerzas armadas convencionales, otros sostienen que los daños causados a la forma de vida de la población pueden ser tan grandes que se justifica el uso de fuerzas convencionales contra ellos. Así se entra en un terreno muy ambiguo: no está claro si los daños que se pueden causar a un Estado en un ataque cibernético serían de tal magnitud que entrasen dentro de lo que el sistema internacional denomina como Derecho Humanitario que protege a los no combatientes. En lo que sí se está de acuerdo es que los Estados en forma aislada no podrán protegerse, de forma tal que las alianzas internacionales en este campo son inevitables, si es que se pretende alguna eficacia.

[8] Una *puerta trampa* es una parte del software de una computadora que se usa para administrar redes. Permite que un usuario externo tenga acceso a una computadora, sin que su propietario se entere.
[9] En idioma inglés, *sniffer*. Es un programa de computación o una parte del hardware de una computadora que puede interceptar y registrar parte de las trasmisiones de una red digital o parte de las actividades de una red. Son programas que permiten que un usuario externo intercepte y grabe datos de una red como claves de usuarios, números de tarjetas de crédito, etc.
[10] Clauswitz Carl, De la Guerra, Edición del Ministerio de Defensa Español, traducción de la edición de la Universidad de Princeton, Madrid, 2002 Libro VI Cap 1.

Contra estas conclusiones básicas conspiran varias realidades: las innovaciones tecnológicas informáticas se renuevan día a día, el hardware de tecnología de información es cada vez más pequeño, portátil y potente, y es de uso predominantemente civil; el control de armas informáticas no podría aplicarse a actores no estatales individuales u organizados. De forma tal que a pesar del atractivo de encuadrar estas actividades dentro de las normas del derecho internacional, se debe ser consciente que ese derecho no va a ser capaz de mantenerse lo suficientemente ágil y versátil para enfrentar los cambios tecnológicos, y por lo tanto nada podrá reemplazar a la vigilancia, la preparación y el ingenio de aquellos que la deban enfrentar.

Las diferencias con otros ataques

Cualquiera sea la consideración, aparentemente algunas de las nuevas formas de ataque son cualitativamente diferentes a las formas anteriores de ataque. En primer lugar, el anonimato, que es la primera gran ventaja de las operaciones cibernéticas: aunque los ataques puedan parecer originados en las computadoras y redes de un Estado, eso necesariamente no significa que este Estado esté involucrado en tales acciones. Si el ataque cibernético es seguido por el uso de fuerzas convencionales, allí recién se podrá identificar fehacientemente al atacante y defenderse conforme al *jus ad bellum,* pero no antes. En segundo lugar, los actores atacantes, que pueden ser gubernamentales o no gubernamentales; civiles o militares; en tercer lugar porque las herramientas que se usan son diferentes, de físicas a intangibles electrónicas; en cuarto lugar por los efectos que causan, unos de destrucción física y ocupación del territorio, otros ataques conducidos a distancia sin necesidad de invasión física; esta vez los daños que se ocasionan pueden variar de la muerte de civiles o militares producto del mal funcionamiento de sistemas de gobierno o militares importantes, el esparcimiento del pánico, el sufrimiento económico, o meramente la interrupción del bienestar en la población civil, la que depende de los sistemas de información para la vida diaria.

Sin que el listado sea completo, aquí se mencionan algunos ejemplos: la introducción de una trampa en el código de control en la red pública, que puede causar fallas a voluntad; un requerimiento simultáneo masivo por medio de robots informáticos a una página web o al sistema telefónico local para hacerlo colapsar; una "bomba lógica" o cualquier otra intrusión en

el sistema de control del tránsito ferroviario que puede causar accidentes, desvío de rutas o choques; tomar el control electrónico de una red televisiva o radial y luego usarla para difundir información errónea; una intrusión en computadoras que automáticamente dosifiquen componentes de medicamentos, o información médica personal, como el tipo de sangre, en las bases de datos informáticos; un ataque preparado por correo electrónico para paralizar una red; una intrusión para desviar fondos en un banco, o corromper la base de datos, cuyo efecto sea que el banco deba temporariamente cerrar [11]; una intrusión para revelar sitios confidenciales personales, civiles o militares, médicos o financieros, que puede ser usado como método de soborno, extorsión o sobresaltos en la vida diaria; el uso de malware en el tráfico de computadoras, que dañe datos e interrumpa sistemas, o impida las migraciones propias de las necesidades de viajes internacionales, o cause que los canales de comando de infraestructura crítica se interrumpan, o interfiera con el sistema de control del tráfico aéreo.

También es comprensible que los Estados delegue la defensa cibernética en las Fuerzas Armadas: sus efectos pueden afectar los intereses vitales de una nación. Pero ello confunde más el escenario el hecho que en las operaciones cibernéticas, aquél que esté en condiciones de defenderse, está en condiciones de atacar. De tal manera, la proliferación de Centro de Defensa cibernética en varios países cuya responsabilidad ha sido depositada en las Fuerzas Armadas que son órganos *de jure* de los Estados, como Estado Unidos, Rusia, China, Israel, Italia, el Reino Unido, Australia y Brasil solo incrementan las sospechas sobre las reales intenciones. Se trata de una nueva arma que por sus efectos ya se califica como de destrucción masiva. Las corporaciones tecnológicas que implementan las decisiones estratégicas cibernéticas de un Estado no son órganos *de jure*, pero el Estado es responsable de sus contratistas de defensa si se prueba que el Estado tuvo un papel en organizar, coordinar, planificar y financiar su acción.

El Derecho Internacional.

[11] El 8 de Marzo de 2011 los diarios publicaron que Francia había sufrido un ataque cibernético. El Ministerio de Economía y Finanzas informó de un ataque que logró infiltrar durante varias semanas unas 150 computadoras de dos áreas cruciales: la de los servicios del Tesoro -que también es responsable del Club de París- y la base de datos del G-20. Noticia publicada en Link http://www.lanacion.com.ar/1355666-el-gobierno-de-francia-victima-de-un-ciberataque

La primera consideración es que todo el cuerpo legal internacional actual está referido a la dimensión geográfica y soberana del territorio, y a sus ámbitos terrestre, marítimo y aéreo. Cuando en la segunda mitad del S XX la humanidad incursionó en el espacio, fue agregado como ámbito, que teóricamente debe ser usado con fines pacíficos y donde ningún Estado puede reclamar soberanía.[12] El espacio exterior es parte del espectro cibernético, porque puede usar los satélites en sus telecomunicaciones.

El derecho internacional regula la interacción entre las naciones y obliga a los signatarios. El derecho internacional consiste en el derecho convencional y en el derecho consuetudinario. El derecho convencional está hecho de tratados y otros acuerdos explícitos entre las naciones, por ejemplo el Tratado de No Proliferación de Armas Nucleares o el Acuerdo General de Tarifas y Comercio. El derecho consuetudinario resulta de la práctica general y consistente entre los Estados. Es el derecho no escrito, basado en la costumbre jurídica, que sienta precedentes. La costumbre internacional es que el derecho consuetudinario requiere de la repetición de una conducta por largo tiempo para que sea considerado como tal. Un ejemplo civil es la Constitución no escrita de Inglaterra; ejemplos militares de derecho consuetudinario son el uso del enmascaramiento para eludir la observación enemiga, o el corte físico de las comunicaciones, o los ataques militares contra sistemas de observación, puestos de vigilancia, estaciones de radar que son aceptables en el derecho Internacional consuetudinario por ser aplicadas desde hace larguísimo tiempo.

Los técnicos sostiene que al día de hoy, los únicos que poseen la capacidad de llevar a cabo ataques cibernéticos masivos sobre un Estado son otros Estados. Si se atribuye tal conducta a Estados, un ataque cibernético es una violación al principio consuetudinario de la no intervención, donde cada Estado resuelve libremente en función del principio de soberanía. Sin embargo, esto está también en discusión, cuando desde el 2005, las Naciones Unidas enunciaron el derecho de injerencia para casos de genocidio, los crímenes de guerra, la depuración étnica y

[12] *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies,* parte del Derecho Internacional sobe el Espacio, entró en vigor en 1967. Se lo conoce vulgarmente como El Tratado del EspacioExterior. A la fecha, ha sido ratificado por 101 Estados.

los crímenes de lesa humanidad[13], pero que es fácilmente ampliable e interpretable a otro tipo de injerencias que siempre estarán en manos de los Estados más poderosos, quienes son los que propiciarán un derecho internacional que satisfaga sus intereses. Acaso un ataque cibernético, ¿No puede ser considerado un crimen de guerra desde que afectará a no combatientes?

Además de estas diferencias, el derecho internacional difiere del derecho interno de cada Estado en que no existe fuerza policial internacional que haga cumplir sus disposiciones. En todo caso, los países que vulneren el derecho internacional están sujetos a las consecuencias políticas y diplomáticas de sus actos. La excepción la constituye los casos de delitos de lesa humanidad establecidos en el Estatuto de Roma y el establecimiento de una Corte Penal Internacional, en vigencia a partir del 1 de Julio de 2002 luego de haber sido firmado por 60 países, donde en el Artículo 24 se aclara que "*Irretroactividad ratione personae*: 1. Nadie será penalmente responsable de conformidad con el presente Estatuto por una conducta anterior a su entrada en vigor."

Las nuevas tecnologías de información que han traído sobre la mesa el tema cibernético, plantean entonces un desafío legal. El primer escollo es que hasta este momento, los daños físicos causados por armas o guerras tradicionales pueden verse de inmediato, en tanto que los ocasionados por armas cibernéticas son intangibles en su acción, pero tangibles en los eventuales daños. El segundo consiste en que las señales informáticas causantes de ataques informáticos no reconocen el principio de soberanía territorial y pueden provenir de terceros Estados, organizaciones o individuos que no estén dentro del ámbito soberano de los Estados involucrados, y que pueden usar el hardware y medios de otro Estado como trampolín debido a la globalización de las comunicaciones. A pesar de ello, cada Estado ejerce su soberanía de los medios de informática y telecomunicaciones dentro de su frontera. Finalmente, los ataques cibernéticos son difíciles de categorizar a la usanza de los conceptos vigentes de paz o guerra. Por lo tanto, es difícil aplicar el concepto de combatiente y no combatiente y escapa a los conceptos del DICA sobre protección de los no combatientes, donde se distingue claramente los blancos militares de los blancos civiles.

[13] UN Res A/60 L.1 del 15 Septiembre de 2005, Documento Final de la Cumbre Mundial 2005, párrafos 138 y 139 obtenible en http://www.cinu.org.mx/cumbre2005/Cumbre_Mundial_2005_files/documento%20final.pdf fecha de consulta 20 Abril 2013.

La novedad tecnológica cibernética y el derecho vigente en telecomunicaciones.

Debido a la novedad de la tecnología empleada, el derecho internacional no prohíbe lo que ahora se conoce como guerra informática. Si nos atenemos a una regla cruda, todo lo que el derecho internacional no prohíbe, está autorizado. No obstante la novedad, el derecho internacional existente se refiere a muchas técnicas de la información en diversas circunstancias, conforme al Derecho Internacional de las Telecomunicaciones.

Cualquier ataque a redes y telecomunicaciones puede involucrar a la Unión Internacional de Telecomunicaciones (UIT) que es el organismo especializado de telecomunicaciones de la ONU encargado de regularlas a nivel internacional entre las distintas administraciones y empresas operadoras. Tiene su sede en Ginebra. La Convención Internacional de Comunicaciones se aplica a las comunicaciones alámbricas y radio frecuencias. En la práctica, la UIT podría no limitar sustancialmente las actividades de guerra informática.

La principal preocupación de la UIT es la interoperabilidad y la interferencia. Uno de los conjuntos de regulaciones iniciales para comunicaciones radiales requería interoperabilidad de los sistemas marítimos, después que varios incidentes peligrosos tuvieran lugar en el mar, porque la Compañía Inalámbrica Marconi tenía el derecho exclusivo para instalar y operar los sistemas radiales en buques, y habían rehusado permitir a los operadores comunicarse con cualquier otra estación que no tuviera los equipos Marconi. Se dice que la tragedia del Titanic podría haber sido evitada, o la mayor parte de sus víctimas podría haber sido rescatada de no ser por el monopolio Marconi.

La UIT y sus normas promulgadas bajo su amparo tienen alguna aplicación en los ataques informáticos que usen el espectro electromagnético o las redes internacionales de telecomunicaciones. La emisión de estaciones de un país no deben interferir con las emisiones de otras estaciones de otros países que operen en las frecuencias autorizadas; para eso, la Junta Internacional de Registro de Frecuencias (IFRB) administra el espectro radioeléctrico a nivel internacional para resolver los problemas relacionados de una manera neutral. Eso se lleva a cabo para prevenir las interferencias. Aún las instalaciones militares deben observar los

requerimientos de no interferencia. Además, las estaciones de radio costa afuera están prohibidas, y los Estados no pueden llevar a cabo trasmisiones de señales falsas o engañosas. Asimismo, los gobiernos deben proteger el secreto del intercambio internacional, aunque retienen el derecho de impedir las trasmisiones de radio o alámbricas por propósitos de seguridad nacional e interna. Esta cláusula está hoy bajo revisión, para los casos en que se trate de competencia en política interna y libertad de expresión.

Parecería que estas previsiones podrían evitar la interrupción de las telecomunicaciones de un adversario, pero en la práctica no lo hacen. En primer lugar, las reglas contra la interferencia no se aplican a beligerantes, por lo que las comunicaciones en tiempo de guerra son justas. En segundo lugar, y aún en tiempo de paz, la violación de normas de la UIT puede tener una repercusión limitada, en especial cuando se trata de un país importante en telecomunicaciones. Por lo expresado, la Junta Internacional de Registro de Frecuencias es más un cuerpo de coordinación antes que una agencia regulatoria, ya que no hay una entidad internacional para hacer cumplir sus decisiones.

Es interesante ver que la Carta de ONU, redactada hace más de 60 años, expresa en su Cap. VII Acción en casos de amenaza a la paz, quebrantamiento de la paz o actos de agresión, en su Art. 41 dice: "El Consejo de Seguridad podrá decidir qué medidas que no impliquen el uso de la fuerza armada han de emplearse para hacer efectivas sus decisiones, y podrá instar a los Miembros de las Naciones Unidas a que apliquen dichas medidas, que podrán comprender la interrupción total o parcial de las relaciones económicas y de las comunicaciones ferroviarias, marítimas, aéreas, postales, telegráficas, radioeléctricas, y otros medios de comunicación, así como la ruptura de relaciones diplomáticas". [El subrayado es nuestro].

El escenario se ha complicado más con la aparición del uso del espacio para las telecomunicaciones. El derecho internacional en el espacio da un amplio espacio para la guerra informática. En especial, el Trato del Espacio Exterior, (1967) cuyo nombre completo es "Tratado sobre los Principios que Gobiernan las actividades de los Estados en la Exploración y Uso del Espacio, incluyendo la Luna y Otros Cuerpos Celestes", prohíbe que se use el espacio para armas nucleares o armas de destrucción masiva en la órbita de la Tierra, debiendo ser todos

los usos pacíficos. Luego, la pregunta es si este Tratado autoriza implícitamente el uso de comunicaciones satelitales para guerra informática, dado que no lo prohíbe.

Los acuerdos de la Organización Internacional de Comunicaciones Satelitales (INTELSAT), 1971, y la Convención de la Organización de Telecomunicaciones Satelitales Marítimas (INMARSAT) 1976, también afectan a las telecomunicaciones en el espacio, pero su relevancia se limita a los principios de no discriminación entre las naciones que usen los satélites.

Sin embargo, el espacio puede ser y ha sido usado con propósitos militares. Desde el avión de reconocimiento de alta altura U 2 (1955) que volaba a más de 23.000 metros de altura, a la denominada en la jerga *Guerra de las Galaxias* (Escudo Antimisiles) de la *Strategic Defense Initiative* (SDI) del presidente Reagan en 1980 que supuestamente involucró a la Unión Soviética en una carrera tecnológica que no puedo sustentar, ocasionando su colapso, el espacio ha sido usado para propósitos militares. También, el espacio es usado en forma rutinaria para comunicaciones militares, navegación, y guía de armas inteligentes. De cualquier forma, el significado de "uso pacífico" no está bien definido y por lo tanto, debido a su carácter no letal, no intrusivo físicamente, la guerra informática podría ser considerada "pacífica".

Otro asunto a considerar es si la guerra informática usando comunicaciones satelitales puede ser considerada como un arma de destrucción masiva. Los efectos catastróficos de ataques cibernéticos podrían ser considerados como arma de destrucción masiva, con los mismos efectos de una bomba nuclear. Claro que ello abriría la discusión que tal ataque cibernético usaría las comunicaciones satelitales, pero estaría basado en el terreno y no en el espacio. El satélite en este caso, actuaría como conductor del ataque, de la misma forma si se usa como guiado de un misil estratégico intercontinental.

La Práctica de los Estados en los conflictos convencionales.

La práctica de los Estados, en sí misma una fuente del derecho internacional consuetudinario, parece permitir mucho de lo que se considera guerra informática. Como ya se dijo, el espionaje ha sido practicado desde siempre, aunque universalmente se lo considere un delito bajo las leyes internas de los Estados, en sí mismo no viola el derecho internacional. Más

aún, los sensores orbitales que pueden llevar a bombardear otros territorios con ondas de radar u otras formas de radiación electromagnética es una práctica común, ya que está permitida tanto en la guerra como en la paz.

Las comunicaciones de un adversario son blancos legítimos para ser interrumpidos durante una guerra. Eso ha ocurrido en cables submarinos en todas las guerras navales, inclusive los que conectaban beligerantes con neutrales. Los gobiernos han llevado a cabo interferencias radiales y escuchas, ya sea en paz o en guerra. Finalmente, los ardides han sido parte de la guerra desde hace milenios, Si el Caballo de Troya fue legal y aceptado como forma de hacer la guerra, se podría argumentar por qué los Troyanos informáticos no puedan serlo.

A pesar de la novedad de algunas técnicas de guerra informática, el derecho internacional pone ciertas restricciones al ambiente cibernético, así como lo hace para las formas tradicionales de hacer la guerra. No obstante, las características de la tecnología ponen problemas para aquellos que quieran usar el derecho internacional para ponerles limitaciones, y deja espacio legal para aquellos que quieran usar este tipo de guerra.

La primera limitación de la Guerra Informática concierne a la neutralidad y a la soberanía nacional. En tratados y en el derecho internacional consuetudinario, el territorio de Estados neutrales en un conflicto se supone inviolable. Por lo tanto, aquél que use los medios de informática y telecomunicaciones de un estado neutral infringiría esta norma y podría ser considerado ilegal, y quizás un acto de guerra contra el estado neutral. De la misma forma, un Estado neutral que permita que sus medios de informática y telecomunicaciones sean usados contra un tercer Estado, desde el momento en que la soberanía se ejerce sobre los propios medios, podría perder el carácter de neutralidad y exponerse a represalias.

Este es un punto controversial. Unos sostienen que el Estado es responsable del uso de los medios informáticos y de telecomunicaciones dentro de su territorio, en tanto que otros sostienen que de la misma manera que colocar bases militares o usar espacio aéreo neutral para llevar a cabo ataques sobre un tercer Estado, en sí mismo no constituye un ataque al país neutral, y por tanto un país neutral no tiene obligación alguna en impedir el uso de su equipamiento de comunicaciones que tiene carácter público. Además de que esta prohibición de usar instalaciones militares en países neutrales ha sido groseramente violada en el pasado – véanse los casos de

Portugal, Turquía y Suiza en la IIGM – no es tan obvio si el uso de la computadoras, redes y facilidades de comunicaciones de un país neutral violaría la neutralidad de un Estado, o legalizaría una eventual represalia de algún beligerante. El principal problema se encuentra en que no existe derecho internacional que legisle sobre la forma en que se debe comportar un Estado neutral en época de paz. [14]

En cuanto al Derecho Internacional Humanitario, tampoco es obvio que todos los daños que podrían causarse traten de las heridas que protege el Derecho Internacional Humanitario. El cuerpo principal del Derecho Internacional Humanitario es que los métodos posibles de dañar al enemigo no son sin límites, y que la crueldad en la guerra debe ser mitigada y circunscripta. El principal mandato es el de proteger a los no combatientes civiles. Bajo la Convención de la Haya, las fuerzas militares no pueden atacar ni bombardear ciudades indefensas, viviendas o edificaciones. Esto ha sido groseramente violado, y juzgado únicamente al vencido – véase el bombardeo de Hamburgo por parte de los aliados en la II GM, o más recientemente, en caso de la ex Yugoslavia. Sin embargo, lo que no está claro es la interrupción de sistemas bancarios, o sistemas de información confidencial, o sistemas de información personales, constituye esa clase de heridas a las que se refiere el derecho Internacional Humanitario. Por otro lado, en todas las guerras la población sufre penurias dentro del marco legal, como la imposición de embargos económicos contemplados en la Carta INU, Cap. VII.

El uso dual civil-militar de muchas redes de telecomunicaciones y equipamiento, sumado a la interdependencia e interconectividad de los sistemas civiles y militares, complica la aplicabilidad del Derecho Internacional para restringir la Guerra Cibernética. Este uso dual es el que esfuma la distinción entre sistemas militares y civiles, y en consecuencia, entre blancos militares legítimos y blancos civiles ilegítimos. No hay distinción lógica entre sistemas tecnológicos militares y civiles, luego no existe una distinción técnica en la selección de blancos ni diferencia entre ataque o defensa en el campo de la Guerra Cibernética.

¿Es guerra o no es guerra?

[14] Documento ONU AG 40 553, Conceptos de seguridad, 1986, párrafo 39 P. 10 "There are no rules of international law concerning how a neutral State must act in peace-time".

El problema es que un efecto lateral de la tecnología informática no está contemplado en categorías legales. Más aún, si se habla del espacio, no muchos Estados pueden aplicar sus recursos en el ámbito cibernético, de forma tal que cualquier limitación del derecho internacional que se quiera establecer es únicamente teórica para los menos desarrollados, por lo que deviene en abstracto para algunos. Los estados poderosos pueden aplicarlo o dejarlo de aplicar a voluntad.

Quizás la clave pasa por definir qué significa "fuerza", ya que el uso de tal como agresión está prohibido en la relación entre estados. Si se define fuerza como poder, violencia o presión dirigida contra una persona o una cosa, o si le damos el significado de la lengua castellana *Aplicación del poder físico o moral* o *Acto de obligar a alguien a que asienta a algo, o a que lo haga*, [15] un ataque cibernético es una agresión, y por tanto, la definición de Agresión de la UN Res 3314/74, debería ser actualizada. Sin embargo, en la Carta ONU en muchos lugares se agrega el adjetivo "armada" a la palabra fuerza, pero en el Artículo 2, se habla de *liberar a las generaciones futuras del flagelo de la guerra*, sin incluir otras formas de coerción.

No obstante, el término fuerza *armada* también da lugar a interpretaciones: *armada* deviene de *arma*, y pudiera no restringirse a un tipo específico salvo que se usa para imponer el poder. Ese es el concepto ya adoptado respecto a las armas químicas y biológicas, las que se incluyen en la categoría de Armas de Destrucción Masiva. Si las armas químicas y biológicas son calificadas como armas, ¿Por qué no pueden serlo las armas cibernéticas, si se usan con intención hostil? Si esto es así, la fuerza cibernética de un estado es otro tipo de Fuerza Armada.

Si se incluye los ataques cibernéticos como guerra, aunque un ataque cibernético mediante *hackeo* o *malware* puede ser parte de ella, no es tan claro que esos actos puedan ser calificados como actos de guerra, porque no son letales, ni son físicamente destructivos, aunque pueden causar disturbios severos y sufrimientos en la población civil. La guerra, como siempre se entendió, incluye fuerzas armadas, y violencia física. La prohibición de la guerra se aplicó siempre únicamente a la fuerza física, y esa fue la intención de la Carta ONU cuando fue redactada. No obstante, en esa oportunidad, Brasil propuso incluir "medidas económicas" al concepto de "uso de la fuerza", pero su propuesta fue rechazada. Es así como el Art. 51 de la

[15] Diccionario de la Real Academia Española, obtenible en http://www.rae.es/drae/ fecha de consulta 18 Abril 2013.

Carta ONU reconoce el derecho de un Estado de usar la fuerza en defensa propia contra un ataque armado.

Asimismo, la definición de "agresión" hecha por la Asamblea General en 1974 [16]revela un enlace de este concepto con poder militar o fuerzas armadas. Otras prácticas legislativas de las Naciones Unidas muestran que el concepto de "agresión" está ligado a las fuerzas armadas. Cabe preguntarse si los conceptos de agresión de tal resolución aún se mantienen vigentes, ya que fueron expresados en plena Guerra Fría. Por de pronto, no se ajustan a la denominadas nuevos riesgos estratégico trasnacionales para los Estados, que atraviesan las fronteras geográficas, y no son aplicables al concepto de seguridad y defensa cibernética, ni al terrorismo internacional, ni al narcotráfico ni a las migraciones descontroladas ni a ninguna otra amenaza trasnacional de hoy, reconocidas por las Naciones Unidas.

Ayudaría a clarificar el panorama si Naciones Unidas volviera a definir el concepto de agresión de la UN Res 3314/1974, actualizado a las necesidades del mundo hoy. Si así lo hiciera, la seguridad cibernética ocuparía un lugar allí, con implicancias para la defensa nacional. En 1953, Irán propuso que las Naciones Unidas entendieran que cualquier acto de un Estado que sirviera al mismo propósito de un ataque armado o que involucrara coerción que pusiera en riesgo la independencia, fuera considerado también un acto de agresión, pero esta interpretación no fue adoptada en Naciones Unidas.

Aunque lejos de ser imaginado en la época en que se redactó, la Resolución AG 2131/ 1965 [17] en su párrafo 1 establece que: *1. Ningún Estado tiene derecho de intervenir directa o indirectamente, y sea cual fuere el motivo, en los asuntos internos o externos de cualquier otro. Por lo tanto, no solamente la intervención armada, sino también cualesquiera otras formas de injerencia o de amenaza atentatoria de la personalidad del Estado, o de los elementos políticos, económicos y culturales que lo constituyen, están condenadas.* Puede cuestionarse su validez, en función de que la tecnología informática en esos momentos no estaba desarrollada al punto de

[16] AG Res 3314 (XXIX) Diciembre 1974 Anexo.
[17] Ag Res 2131, 20th Sess. Supp Mro. 14, obtenible en http://www.dipublico.com.ar/3975/resolucion-2131-xx-de-la-asamblea-general-de-las-naciones-unidas-declaracion-sobre-la-inadmisibili-dad-de-la-intervencion-en-loa-asuntos-inter%C2%ADnos-de-los-estados-y-proteccion-de-su-inde%C2%AD/, consultada el 08 de Abril de 2013.

poder usar el espacio cibernético para llevar a cabo las acciones mencionadas. Esto es una clara indicación que debe legislarse nuevamente.

En suma, si la distinción existente entre el uso de la fuerza física e infringir sufrimiento por medios cibernéticos es legalmente válida, los ataques informáticos no violentos pudieran ser considerados actos de no guerra, y luego podrían no estar sujetos a las restricciones legales que gobiernan al fenómeno social guerra. Surge también de esto que si el Derecho Internacional Humanitario no se aplica en el ámbito cibernético, luego los Estados pueden emprender acciones de ataque cibernético sin preocupación por los sufrimientos que podría inferirse a la población civil. Sin embargo y aquí aparece la contradicción, muchos ataques informáticos pueden ser considerados amenazas a la paz y seguridad internacionales y por lo tanto, puestos a consideración y acción del Consejo de Seguridad. En este caso, nada impide que el Consejo de Seguridad permita el uso de la fuerza armada en respuesta.

El mayor riesgo es el error en la percepción del ciberatacado. No será la primera guerra que se desata por una percepción errónea. El primer dilema es distinguir si una catástrofe ha sido un error de las computadoras natural o accidental surgido de una voluntad en oposición. Errores o conflictos en el software son conocidos o sospechados de haber causado incidentes que pudieran creerse un ataque informático. Un ejemplo ocurrió en el Día de Martin Luther King en 1990, cuando las redes de líneas de larga distancia de AT&T estuvieron inoperables por 9 horas. Aunque finalmente se estableció que fue una falla del software, inicialmente se creyó que hackers habían saboteado las redes. En 1990, un reactor nuclear canadiense lanzó miles de litros de agua radioactiva y finalmente, eso se atribuyó a un error del software. Igualmente, en 1992 una demora en la selección del blanco causó que un piloto de la Real Fuerza Aérea británica lanzara una bomba de ejercicio sobre un portaaviones propio. También se ha sugerido que en un choque entre dos F 117 estadounidenses en circunstancias sospechosas puede haberse debido a un error [en inglés bug] en sus sistemas informáticos.

Por lo tanto, existe un peligro grande que en momentos de tensión y desorden, se confunda un error en los programas con un ataque cibernético. Lo sistemas de discernimiento en el campo cibernético son frágiles. Especialmente los países poderosos van a ser tentados a tomar más decisiones políticas que judiciales, y la diplomacia coercitiva es más atractiva en el

poderoso que los argumentos lógicos. Posiblemente la ONU y la comunidad internacional requerirá pruebas que se trata de un ataque cibernético y no de una falla en los programas, pero probablemente los Estados poderosos rehúsen proporcionarlas para no revelar sus fuentes y sus métodos, o lo expliquen *post facto*, o se disculpen *post facto*.

La próxima cuestión es quién investiga para determinar si se trata de una falla del programa o un ataque cibernético. La dispersión de los medios, la disponibilidad barata de las tecnologías más modernas combinadas con el anonimato [hasta hoy el anonimato en la red no es delito; hay programas de servers anónimos a disposición de quien los solicite en un buscador de internet, aunque ya se requiere identificación si el acceso disfraza el IP de la máquina] pueden complicar las investigaciones. También existen otros sistemas como el *Echelon*, cuyo detalle excede este ensayo, pero que hace espionaje sobre las comunicaciones electrónicas. Según parece, este sistema busca palabras claves en correos electrónicos y permite el seguimiento de tráfico electrónico. Se dice que una manera de engañar a este sistema es mandar mensajes intrascendentes conteniendo esas palabras - siempre que se las conozca - por un lapso más o menos largo, hasta que el *Echelon* descarte la fuente, y así el emisor pueda liberarse de la vigilancia.

Un ataque cibernético puede provenir de un país extranjero, o ser encaminado a través de las computadoras y servidores en diferentes países, pero el personal de seguridad cibernética del país afectado no puede abiertamente investigar las redes de otros países, porque afectaría el principio de soberanía. Por tanto, se necesita de la cooperación internacional, y eso requiere de acuerdos del tipo de la persecución *in itinere* entre gobiernos, lo que va a ser objetado por los partidos políticos que no detenten el poder. Por lo tanto, pocos gobiernos estarán dispuestos a pagar ese precio. Sería fácil en aquellos bloques regionales de larga data y con intereses comunes, como Canadá y EEUU, o la UE, pero más difícil en otros sitios del planeta.

El conflicto entre las redes internacionales y el espacio cibernético y las soberanías nacionales no es un asunto puramente académico. Hasta ahora se ha recurrido al pedido de extradición de los agresores cibernéticos de otros países, pero no todas las legislaciones nacionales contemplan tal posibilidad. El mero concepto de no cooperación no es indicativo cierto de prueba de estar implicado en un ataque cibernético. Aunque algunos Estados no hayan

estado involucrados en un ataque cibernético, o aunque muestren simpatía por él, o no deseen cooperar, eso no significa que estén necesariamente involucrados. Hasta algunos gobiernos pueden desistir de cooperar con el Estado demandante por razones de política interna.

A esto se suma una tensión natural que existe aún en los Estados poderosos: la investigación de ciudadanos en nombre de la seguridad de la nación se contrapone con los derechos individuales de privacidad. Es probable que la privacidad sea la que pierda en esta tensión, pero esto sería una herramienta muy peligrosa en manos de gobiernos inescrupulosos.

Un caso paradigmático reciente es el pedido de extradición del responsable de *Wikileaks*, que penetró archivos y mensajes confidenciales de varios lugares. *Wikileaks* es una organización internacional sin fines de lucro que a través de su sitio web publica informes y documentos con contenido clasificado, preservando el anonimato de sus fuentes. Su creador es un australiano, Julián Assange. Desde Noviembre del 2010 Assange tiene una orden de arresto emitida por el Reino Unido, pero desde el 2012 se encuentra asilado en la Embajada del Ecuador en Londres, donde pidió asilo político, que le fue otorgado porque en Ecuador el delito por el que se lo acusa no está tipificado. Hasta el 2010, los servidores de los proveedores de Servicios de Internet de Wikileaks estaban en Suecia, porque allí en la legislación nacional se prohíbe revelar las fuentes de información.

Este es el complicado panorama que se presenta en la identificación y acusación ante tribunales de justicia de organizaciones cibernéticas que afectan la seguridad de los Estados. Las facilidades de informática y telecomunicaciones son globales, los ataques cibernéticos pueden lanzarse de cualquier lugar del planeta pero las legislaciones nacionales no son uniformes. ¿En cuántos de los casi 200 países que componen Naciones Unidas se considera la intrusión informática un delito? Aplicar la extradición por ataques cibernéticos requiere que eso sea tipificado delito en ambos Estados, el que requiere la extradición y en el que la otorga. Igualmente, si un Estado no quiere extraditar a un acusado, puede apelar a muchísimas formas de no hacerlo, buscando vericuetos legales, ello a pesar de ningún acuerdo. Algunas naciones pueden tener razones ideológicas, o diferentes conceptos de privacidad en sistemas o datos electrónicos, o desconfianza de los sistemas que preserven los intereses de los Estados más poderosos.

Estas diferencias de criterio probablemente causen – como en el caso de *Wikileaks* mencionado – que los hackers o las organizaciones delictivas o terroristas o narcotraficantes se desplacen a aquellos países donde la legislación les sea más favorable. También es más probable que esta legislación tolerante se encuentre en países con menos desarrollo informático, y los gobiernos vean en ello una oportunidad para importar capital humano que pueda ser usado contra sus enemigos más poderosos, o por lo menos para mejorar su estructura informática.

Los recursos legales y los recursos de fuerzas convencionales

El primer recurso legal sería recurrir al Consejo de Seguridad de las Naciones Unidas, siempre que el atacado pueda identificar fehacientemente que tal ataque proviene de otro Estado, conforme lo establece el Art 35 inciso 1, bajo el Arreglo Pacífico de Controversias. Allí, el Consejo de Seguridad determinará si se trata de una amenaza la paz, un quebranto de la paz o un acto de agresión, y so va hasta la aplicación del Capítulo VII Acción en caso de amenazas a la paz, quebrantamientos de la paz o actos de agresión. La categoría sin discusión será que al menos, se trataría de una amenaza a la paz. Otra forma es que el Consejo de Seguridad recurra al artículo 41, aunque hoy respecto a la interrupción de las comunicaciones radioeléctricas con el Estado agresor, tiene poca aplicación debido a la globalización, aunque puede interpretarse la figura de bloqueo cibernético, aunque no esté así mencionado.

El otro recurso legal podría ser llevar el caso a una Corte Internacional, como lo sería la Corte Internacional de Justicia. Tendría la demora propia en arribar a una recomendación, además que las resoluciones no son mandatarias para los Estados.

Algunos autores sostienen que la responsabilidad de un Estado no exime de la responsabilidad delictiva de los individuos u organizaciones que hayan llevado a cabo un ataque cibernético. En el año 2010 se llevó a cabo un Uganda una Conferencia de Revisión del Estatuto de Roma, que adoptó el modelo de agresión de la UN Res 3313/74, pero excluyó el Art 4 de esa Resolución que dice: *La enumeración de los actos mencionados anteriormente no es exhaustiva y el Consejo de Seguridad podrá determinar qué otros actos constituyen agresión, con arreglo a las disposiciones de la Carta.* Sin embargo, la responsabilidad recae en quienes dirijan la acción política o militar de un Estado, y no en los que la ejecutan. Aquí se encuentra una penumbra

legal si se quiere aplicar a la guerra cibernética, por ejemplo si un *hacker* dirigiera misiles balísticos intercontinentales.

Dentro de las medidas pacíficas, también podría incluirse la retorsión y las contramedidas no militares, pero se entra en el terreno gris del uso de ataques cibernéticos como defensa. Retorsión es la acción de devolver o inferir a alguien el mismo daño o agravio que de él se ha recibido, y eso no excluye al ataque cibernético para divulgar códigos maliciosos en las computadoras y redes que hayan llevado a cabo el ataque, aunque los servidores se encuentren en un tercer país.

En el Derecho Internacional de Guerra, las represalias están prohibidas. Están prohibidas las represalias contra las personas civiles; los prisioneros de guerra; los heridos, los enfermos y los náufragos; el personal sanitario y religioso y los respectivos equipos; los edificios, los equipos y las embarcaciones protegidas; los bienes de carácter civil; los bienes culturales; los bienes indispensables para la supervivencia de la población civil; las obras que contienen fuerzas peligrosas; y el medio ambiente natural. [18] Como último recurso, cuando hayan fallado todas las demás medidas tomadas, se puede decidir, al más alto nivel político (no miembros de las fuerzas armadas), tomar represalias con la única finalidad de hacer que el enemigo aplique el derecho de los conflictos armados. Se puede tomar represalias solo si: la finalidad es conseguir que la guerra se haga de conformidad con el derecho; hay aviso previo por lo que respecta a la intención de tomarlas; son proporcionadas con respecto a la alegada violación por parte del enemigo; y cesan tan pronto como cese la alegada violación por parte del enemigo; y han sido ordenadas a nivel gubernamental.

El uso de las fuerzas armadas convencionales contra ataques cibernéticos nos refiere al Arto. 51 de la Carta ONU, que dice *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 que el Consejo de Seguridad haya tomado las medidas necesarias para mantener la paz y la seguridad internacionales. Las medidas tomadas*

[18] I Convenio de Ginebra, artículo 46, II Convenio de Ginebra, artículo 47, III Convenio de Ginebra, artículo 13, IV Convenio de Ginebra, artículo 43; Protocolo adicional I a los Convenios de Ginebra, artículos 20, 51, 52, 53, 54, 55 y 56.

por los Miembros en ejercicio del derecho de legítima defensa serán comunicadas inmediatamente al Consejo de Seguridad, y no afectarán en manera alguna la autoridad y responsabilidad del Consejo conforme a la presente Carta para ejercer en cualquier momento la acción que estime necesaria con el fin de mantener o restablecer la paz y la seguridad internacionales.

De su lectura surge que debe existir un ataque armado y cabe preguntarse si se refiere a armas específicas o al uso de la fuerza no solamente física. Lo que hace que algo se transforme en arma es la intención con que se use. Los lectores se asombrarían de cuántas cosas de uso diario podrían constituir un arma. Por ejemplo, en el ataque a las Torres Gemelas, las armas usadas para perpetrar el terrorismo catastrófico fueron dos aeronaves de uso civil, y ONU reconoció el derecho de la defensa propia individual o colectiva.[19]

. El Derecho Internacional por elaborarse debería contemplar magnitudes de un ataque cibernético que ameritarían el uso de la fuerza convencional: no sería lo mismo un ataque DDoS que podría ser considerado uso de la fuerza pero que no causase daños significativos, que otros ataques cibernéticos que buscaran muertes por la anulación de computadoras que regulen servicios esenciales, anulación absoluta de grillas eléctricas que causen daños extensos a la vida diaria, daños que puedan ser causados al control informático del funcionamiento de represas que puede causar inundaciones, o de centrales de energía nuclear que puedan causar emisiones radioactivas, afectación del control de tráfico aéreo que puede ocasionar accidentes con pérdida de vidas, y la destrucción temporal del ejercicio de la autoridad gubernamental.

Su un ataque convencional llevado a cabo sobre una instalación civil de un Estado por otro Estado amerita que se usen fuerzas convencionales para repelerlo aunque no se hayan producido bajas militares, no existe razón lógica por la cual un ataque cibernético sobre un sistema civil que no haya producido bajas militares no pueda repelerse con armas convencionales.[20] Un caso particular sería cuando el ataque en defensa propia se llevara a cabo sobre un tercer Estado al que se le haya usado sus sistemas informáticos y de comunicaciones como puente.

[19] Un Res 1368/2001 obtenible en http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N01/533/82/PDF/N0153382.pdf?OpenElement fecha de consulta 20 Abril 2013.
[20] Caso referido por Marco Roscini.

Si se incursiona en el *jus ad bellum*, debe también hacerse en el *jus in bello*. La forma de conducir una guerra comprendidos en el *jus in bello* comprende dos aspectos: la *proporcionalidad*, es decir que la respuesta a una agresión no debe exceder la naturaleza de tal agresión; y *discriminación*, vale decir que la respuesta debe dirigirse hacia el agresor injusto y no contra gente inocente. Para cumplirlo, será necesario determinar con exactitud al autor del ataque cibernético, verificar previamente que no haya sido un accidente y que la respuesta no pueda ser menos agresiva que un ataque convencional. En cuanto a la proporcionalidad, también es difícil de determinar por asimetrías tecnológicas ya sea en el atacante o en el atacado. Lo más difícil es la discriminación, porque las tecnologías informáticas son de uso dual. El ultimo propósito de la defensa propia no es una represalia contra el atacante, sino el de repeler el ataque.

El ataque preventivo con fuerzas convencionales ante la inminencia de un ataque cibernético aceptará los argumentos del Estado más poderoso. Al mismo tipo que Irak en la invasión aliada del 2003, con el argumento de desarmar a Irak de Armas de destrucción masiva, una vez finalizado el ataque preventivo por causas cibernéticas, el Estado poderoso podrá esgrimir cualquier excusa para justificar la falta de pruebas de las causas que se esgrimieron para atacar preventivamente.

No hay derecho internacional consuetudinario respecto a la guerra cibernética, por su reciente aparición. La opinión sobre esto no es general, porque que sostienen que aunque el período sea corto, no necesariamente impide que se forme un derecho consuetudinario, Por ejemplo, ya hay varios Estados – los poderosos - que han definido lo que entienden por defensa propia en caso de un ataque cibernético, pero para que sea consuetudinario, debería ser un concepto extensiva y virtualmente uniforme, lo que se buscó en la Conferencia de Varsovia de Octubre de 2012. Sin embargo, algunos juristas sostienen que la opinión consensuada mayoritaria debe ser de los que tienen capacidad informática, sin importar la de los que no la tienen, porque se transformaría en una herramienta política que devendría en abstracto, al igual de lo que ocurre con el uso del espacio.

Conclusiones

El progreso tecnológico ha hecho que el ámbito de la Informática y las Telecomunicaciones sea un riego estratégico real para los Estados. El fácil acceso a este tipo de

tecnología, su uso dual civil-militar, el equipamiento barato, la carencia de fronteras en el espacio, los cambios permanentes en la tecnología que crean nuevas vulnerabilidades, y el anonimato; su uso indiscriminado por hackers adolescentes, delincuentes, terroristas, espionaje, robo de datos y agresiones inter estatales, solo agudizan el problema.

Para enfrentar este riego estratégico los Estados deben cooperar, ya que no se los puede hacer aisladamente. Al igual que con el espacio exterior, el desarrollo tecnológico de los Estados es diferente, y se debe evitar un desarrollo de capacidades fuera de control. Los Estados pueden cooperar en transparencia de sus ámbitos informáticos, medidas de confianza mutua, desarrollo de medios simétricos para combatir los riesgos, y una legislación nacional coherente con la internacional.

Para instrumentar la postura de un Estado frente a la agresión cibernética, el primer punto a definir que se reflejará en la organización será la tensión entre los derechos individuales y la injerencia del Estado en la seguridad. En gobiernos inescrupulosos, siempre existirá la tentación de usar la red para prevenir ataques cibernéticos con propósitos de política interna. Por eso, toda organización que se constituya no deberá estar bajo la autoridad gubernamental, sino que deberá ser una organización apolítica, al mismo estilo que las Cortes Supremas que vigilan que los actos de un gobierno se ajusten a derecho, o los Comités Electorales que verifican la fidelidad de los resultados en las elecciones.

Algunos países han optado por crear un Consejo de Seguridad Nacional, que asesora al presidente. No se lo denomina Consejo de Defensa Nacional para no darle una connotación exclusivamente militar. Dado que el riesgo estratégico es transversal, la organización frente a la amenaza cibernética debe ser civil y militar, pública y privada. En principio se debería contar con un Equipo de Respuestas a Emergencias interdisciplinario, un Equipo contra el Delito Cibernético en sus diferentes formas y tal como se lo defina en la ley nacional, y un Equipo de Defensa Cibernética que se refiera a la infraestructura que deberá definirse como “crítica”.

El segundo paso consistiría en elaborar una Estrategia de Seguridad Cibernética nacional. Es una tarea que requiere coordinación previa con las regionales, para asegurar compatibilidad. Esta estrategia debiera incluir medidas de confianza mutua, y diálogo permanente sobre el

asunto. Las medidas de confianza mutua debieran volcarse en un Libro Blanco de Seguridad y Defensa Cibernética de cada Estado.

El primer fundamento de la Estrategia de Seguridad Cibernética es el que aunque el espectro cibernético no reconozca fronteras, como cada estado es responsable de la operación de los medios de informática y comunicaciones dentro de sus fronteras, no puede permitir que se usen sus instalaciones y medios de telecomunicaciones para dañar los derechos de otro Estado. Así lo establece la UN Res 55/63 del 22 Enero 2001, *Lucha contra la utilización de la tecnología de la información con fines delictivos*[21]. Un segundo aspecto es la definición nacional de qué se considera como infraestructura crítica. Cada país debería enunciar claramente qué constituye una infraestructura crítica, ya que es lo que hay que proteger y defender en caso necesario. Eso también es sensible, pues se devela información que hasta ese momento puede ser confidencial. También los Estados pueden definir su estructura crítica en forma general, por ejemplo sus sistemas y bienes físicos y virtuales, públicos y privados, cuya afectación puede debilitar o destruir la seguridad de la nación, su economía, su salud pública, la vida de sus habitantes o una combinación de ellas. La determinación del significado infraestructura crítica es parecida pero no igual en todos los gobiernos: unos dicen que son la energía, el agua, el transporte, el alimento, las comunicaciones, los servicios del gobierno, los servicios de emergencia, la salud pública y las finanzas. Otros agregan a esta lista los bienes físicos y cibernéticos públicos y privados, la industria de defensa, los productos químicos peligrosos, los servicios postales y el comercio internacional. El concepto nuevo que se discute es que los sistemas de interés nacional van más allá del concepto tradicional de infraestructura crítica y también abarca la disponibilidad de sistemas que afecten la prosperidad económica, la competitividad internacional y bienestar nacional de un país. El problema en determinar la infraestructura crítica de un país reside que mucho de ella se encuentra en manos privadas. En definitiva la protección de la infraestructura cae bajo el dominio de la seguridad nacional, y no hay concepto uniforme sobre la frase seguridad nacional que sea aceptado en todas las naciones.

[21] UN Res 55/63 *Lucha contra la utilización de la tecnología de la información con fines delictivos,* Los Estados deben velar para que en su legislación y en la práctica se eliminen los refugios seguros para quienes utilicen la tecnología de la información con fines delictivos; obtenible en http://www.unodc.org/pdf/crime/a_res_55/res5563s.pdf fecha de consulta 20 de Abril de 2013.

Esta Estrategia deberá ser seguida de Políticas en el campo de interés. Le seguirá la organización para enfrentar a este riesgo; la formación del capital humano en licenciaturas o maestrías de seguridad informática y ciencias de computación en una la alianza con el campo académico de las Universidades; la preservación y conservación delos talentos nacionales; la legislación y normas específicas para las actividades del sector cibernético; la contribución intersectorial entre los componentes del poder nacional para hacer efectiva la seguridad, defensa y disuasión cibernética ya que no hay competencias exclusivas en este ámbito; la prohibición de libre acceso a sitios de internet donde se enseñe *hackeo*; apoyar el control internacional de armas cibernéticas al estilo de las armas nucleares; y colocar fuera de la ley al ataque sobre redes cibernéticas que regulen el funcionamiento normal de infraestructura civil.

Referente a la política internacional sobre ataques cibernéticos, es de esperar que los países poderosos en fuerzas convencionales requieran que la comunidad internacional apruebe el Art. 51 de la Carta ONU que justifique el empleo de fuerzas convencionales en caso de ataque cibernético a su infraestructura crítica. Ello probablemente incluya la defensa preventiva y el ataque preventivo en caso de certeza de inminencia de ataque. Siempre habrá un vericueto jurídico que lo justifique, y siempre habrá otro vericueto jurídico que lo prohíba, por lo que la legalidad o la ilegalidad dependerán del poder relativo del Estado que lo lleve a cabo.

Para el caso de los Estados Unidos, el ataque cibernético a instalaciones y redes militares es equivalente al empleo de armas de destrucción masiva. El Informe público sobre la Estrategia Nacional de Seguridad 2006 (NSSR) establece que "buscar una fuerza futura que asegure una disuasión acorde para amenazas estatales y no estatales incluyendo empleo de ADM, ataques terroristas en los dominios físicos e informáticos y agresiones de oportunidad"[22], lo que es ambiguo y genera muchos interrogantes. Informaciones periodísticas del año 2013 [23]dicen que es el Presidente de los Estados Unidos se reserva el derecho de ordenar el empleo del arma cibernética ya sea ofensiva o defensivamente, al igual que con las armas nucleares. Vale notar que supuestamente, en el año 2010 Estados Unidos e Israel fueron quienes diseñaron el gusano

[22] NSSR 2006,
[23] Sanger D. y Shanker T., *Obama con amplios poderes para ordenar cibertaaques*, artículo del Diario La Nación, Argentina, 5 de Febrero de 2013, link http://www.lanacion.com.ar/1551843-obama-con-amplios-poderes-para-ordenar-ciberataques fecha de consulta 20 Abril 2013.

Stuxnet para que inutilizase las centrales nucleares iraníes. No obstante, la autoría permanece en penumbras.

Por su parte Rusia sostiene que debe existir un Acuerdo de Desarme al estilo del existente para las armas nucleares que prohíba el desarrollo, producción y uso de armas informáticas particularmente peligrosas. También las equipara en sus efectos como ADM y funcionarios rusos han hecho público que las armas cibernéticas no van a ser consideradas una parte no militar de un conflicto, haya o no bajas. Cabe notar que aparentemente fue Rusia la que atacó cibernéticamente a Estonia en el 2007, como represalia por haberse derribado el monumento al soldado soviético de la II GM. Asimismo, uso el arma cibernética como propaganda interfiriendo y propagando información falsa en las páginas web oficiales en la invasión a Georgia, aunque ambos casos esta autoría fue negada.

El Reino Unido, por su parte, considera que un ataque cibernético a su infraestructura crítica será considerado como un acto de guerra. La posición de la OTAN es más ambigua todavía. Si bien en el 2007 Estonia solicitó que se aplicase el Art 5 del Tratado del Atlántico Norte[24], de las reuniones sucesivas todo indica que se recurrirá al Art 4. [25]

Hasta donde se sabe, el país que se opone a la aplicación del Art. 51 de la Carta ONU es China, esta postura se basa en la disponibilidad de lo que denominan *Golden Shield* (Escudo Dorado) para operaciones cibernéticas defensivas, y *Blue Army* (Ejército Enfermante) para operaciones cibernéticas ofensivas. Estados Unidos alega que los ataques informáticos llevados a

[24] Art 5: Las Partes acuerdan que un ataque armado contra una o más de ellas, que tenga lugar en Europa o en América del Norte, será considerado como un ataque dirigido contra todas ellas, y en consecuencia, acuerdan que si tal ataque se produce, cada una de ellas, en ejercicio del derecho de legítima defensa individual o colectiva reconocido por el artículo 51 de la Carta de las Naciones Unidas, ayudará a la Parte o Partes atacadas, adoptando seguidamente, de forma individual y de acuerdo con las otras Partes, las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad en la zona del Atlántico Norte. Obtenible en http://www.ehu.es/ceinik/tratados/14TRATADOSDEALIANZASPOLITICOMILITARES/TAPM142.pdf fecha de consulta 20 Abril 2013

[25] Art 4: Las Partes se consultarán cuando, a juicio de cualquiera de ellas, la integridad territorial, la independencia política o la seguridad de cualquiera de las Partes fuese amenazada, ibídem.

cabo en el año 2012 sobre el prestador *google* y sobre el periódico *The New York Times* provinieron de China, que ha denegado toda responsabilidad.[26]

Las naciones en desarrollo podrían adherir a la aplicación del Art. 51 de la Carta según sean sus intereses de política exterior, pero tal adherencia devendría en abstracto ya que no poseen los medios de llevar a cabo ningún uso de fuerza convencional para responderá un ataque cibernético, y abrirían la puerta para que los Estados poderosos que puedan hacerlo, lo hagan sobre su territorio con la excusa que sus servidores fueron usados de *proxy*. Sin embargo, un ataque cibernético sobre un país en desarrollo aislaría al país del mundo, por lo que alguna precaución habría que tomar con una adecuada Política de Seguridad y Defensa Cibernética nacional, que se apoye en alianzas con otros países.

Las certezas iniciales de un análisis somero es que hay que definir con relativa urgencia si un ataque cibernético debe considerarse equivalente a un agresión armada; que es necesario implementar acuerdos regionales y globales de protección; que al mismo estilo que la protección de los bienes culturales, habrá que alcanzar un acuerdo para proteger por ley internacional las instalaciones cibernéticas nacionales; hasta algunos han sugerido recientemente que la guerra informática puede ser un área donde puedan acordarse control de armas, al estilo de las armas nucleares. Ya se habla de una Guerra Fría Cibernética.

El último aporte ha sido llevado a cabo en el NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) con sede en Estonia, consistente en una publicación denominada El *Manual Tallinn sobre el Derecho Internacional aplicable a la Guerra Cibernética*, cuya versión impresa estará disponible a partir de Mayo de 2013. Este Manual no es un documento oficial, sino expresiones independientes de un grupo de expertos. Aquí, se incursiona en los vericuetos legales de las relaciones entre Estados, estructuras cibernéticas y operaciones cibernéticas, y se determina 95 aspectos legales que podrían regular la guerra cibernética desde el punto de vista del Derecho Internacional..

[26] Geof Dyer y otros, *China military linked to hacking attacks*, publicado en FT.com business news and analysis, February 19, 2013, obtenible en http://www.ft.com/cms/s/0/6b057948-7a5b-11e2-9c88-00144feabdc0.html#axzz2RJuaITJD, fecha de consulta 23 de Abril de 2013.

En todo lo mencionado, el problema básico persistirá, en determinar el origen del ataque y la dificultad para discernir un hacker común o red de hackers con motivaciones anárquicas o idealistas; delincuentes cibernéticos; espionaje entre Estados; espionaje económico; y terrorismo cibernético asociado a actores no gubernamentales. Hoy, en el reino de la cibernética, los expertos en seguridad están lejos de alcanzar consenso en el significado de términos como ofensiva, defensiva, disuasión o leyes de guerra.

No se puede menos que recordar a Tucídides, cuando en su obra *Las Guerras del Peloponeso*, expresara que los Estados poderosos hacen lo que pueden [con su poder] en tanto que los Estados débiles hacen lo que deben [lo que le indican los más poderosos].

Bibliografía:

1. Geenberg Lawrence y otros, Information Warfare and International Law, National defense University, Institute for national Startegic Studies, Washington DC, 1997.

2. Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law* Indiana University, Kelley School of Business; University of Cambridge - Department of Politics and International Studies, April 28, 2009 obtenible en http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1396375 fecha de consulta 15 Abril 2013.

3. Roscini Marco, *World Wide Warfare Jus ad bellum and the use of Cyber Force,* Max Planck Yearbook of the United Nations Law, Vol. 14, P 85-130, impreso en los Países Bajos, obtenible en http://www.mpil.de/shared/data/pdf/pdfmpunyb/03_roscini_14.pdf, fecha de consulta 18 Abril 2013.