Ciberguerra
El nuevo concepto y el nuevo desafío bélico y jurídico

Federico D. Arrué
Departamento de Derecho, Universidad Nacional del Sur
federicoarrue@hotmail.com

Abstract. Actualmente, se suele oír un nuevo vocablo: *ciberguerra*. Internet se ha convertido en un arma y el ciberespacio es un campo de batalla. Esta modalidad de agresión, tiene características propias, entre otras: la posibilidad de hacer anónimo al agresor. El derecho sólo regula esta cuestión con principios generales, originalmente no establecidos para ella. Para prevenir los daños que puede ocasionar este accionar, la comunidad internacional debe reconocerse como tal, y actuar conjuntamente, procurando una preparación logística, pero también jurídica.
Palabras clave: Internet, guerra, agresión, anonimato, vacío legal.
Abstract. Actually, it's common hear a new Word: ciberwwar. Internet hast become in a wearpon and cyberspace it is a battlefield. This mode of agresión has his own features, like the posibility to make anonymous agressor. The Law Orly regule this problema whit general principle. To prevente damages form this actions, the International Comunity must recognise at comunity and act alltogether, to procure a logistic preparation, but also a legal preparation.
Key Words: Internet, War, Aggression, Anonymous, Legal Vacuum

I. INTRODUCCIÓN.

Nadie se asombre de que el término ciber –del griego *cibernao*, que significa *pilotear una nave*- y que se refiere a Internet y todo lo vinculado con ella; pueda verse hoy unido al término *guerra*, para formar el título de este trabajo, que a primera vista parece futurista, pero no pretende más que ser realista y previsor.

Desde tiempo inmemorial, todo elemento que logró dominar el hombre, fue desviado a un fin bélico. La piedra, herramienta fundamental de los humanos primitivos, se utilizó para fabricar armas, no sólo para dar caza a animales, sino también para combatir a otros hombres. El fuego, componente vital en nuestra evolución, sirvió para incendiar poblados y cosechas.

Ya en la modernidad, la dinamita no sólo rasgó la roca y la tierra para abrir túneles y galerías, sino que sirvió para esparcir la muerte en nubes de polvo y estruendo; para desesperación de Nobel. Incluso, algunos descubrimientos fueron originalmente armas militares, y luego se les descubrió un uso provechoso en el ámbito civil del bienestar y el desarrollo. La energía atómica es el ejemplo más claro de ellos.

En el mismo sentido, cada vez que el hombre logró dominar un medio, llevó a él sus elementos bélicos. El mar del transporte de personas y mercancías, fue surcado por buques de guerra, que evolucionaron hasta ser las baterías flotantes de hoy en día. El submarino, se desarrolló tanto para explorar como para combatir, y actualmente son más los submarinos militares que los civiles. El aire, sueño del hombre, reservado mucho tiempo a las aves del cielo, al caer rendido a los pies del genio humano, fue invadido de bombarderos y cazas.

Así pues, nadie se extrañe que el monstruo terrible de la guerra haya llegado al campo cibernético.
Como "ciberguerra" se puede entender el uso Internet como un arma militar –como única arma o como un arma atípica que se suma a otras-. Esto trae como consecuencia que el ciberespacio pase a ser un teatro de operaciones o un campo de batalla.
Sobre esta materia específica, la mayoría de lo que se ha escrito, es crónica periodística. Sin embargo, desde aquí atenderemos fundamentalmente al aspecto jurídico.

II- ALGUNOS EJEMPLOS PARADIGMÁTICOS

El 27 de abril de 2007 se produjeron una serie de ataques cibernéticos que afectaron varios sitios en Internet pertenecientes al gobierno de Estonia, y vitales para él. Los blancos principales fueron la presidencia, el parlamento, los ministerios, los partidos políticos, algunas corporaciones de medios de gran relevancia en el país –diarios y cadenas de televisión-, y dos grandes bancos. Los sitios web de estas dependencias fueron sobrecargados de visitas, que superaron el ancho de banda y produjeron una parálisis masiva de los sistemas.
Estos ataques se producían mientras en Estonia se debatía, de manera por demás polémica, la reubicación de un célebre monumento conocido como "Soldado de bronce de Tallin": un monumento soviético en la capital de Estonia, que rememora la liberación rusa de la ciudad, tomada por los alemanes en la Segunda Guerra Mundial. Es pues, para los rusos y para sus descendientes en Estonia, un símbolo de su victoria sobre el nazismo. Sin embargo, para los estonios, es símbolo de la ocupación soviética de su país.
La reacción inmediata del gobierno de Estonia fue acusar a Rusia de estar detrás del ataque. Posteriormente Estonia admitió que no tenía pruebas para esa acusación. Tampoco organizaciones como la OTAN o la Unión Europea encontraron rastro alguno de Moscú en el incidente. Lo que es claro en cualquier caso, es que una operación de tanta dificultad y tal magnitud requirió sin lugar a dudas un procedimiento por demás sofisticado, que difícilmente se pueda haber llevado a cabo sin el apoyo de un gobierno extranjero. Si, por el contrario, como sostienen otras voces, el procedimiento fue obra exclusiva de opositores internos en Estonia –de tendencia pro-rusa-, estamos frente a un terrorismo cibernético digno de ser tenido en cuenta y considerado susceptible de ser incluido como objetivo en la lucha global contra el terrorismo.

En julio del 2008, varios virus de origen ruso atacaron simultáneamente sitios en la web de la presidencia, el parlamento, algunos ministerios, bancos y agencias de información de Georgia. Esto provocó caos en algunas actividades gubernamentales y en los demás blancos de la agresión, y explayó una serie de mensajes propagandísticos en contra del presidente Mijeil Saakashvili a quien se comparó con Adolf Hitler.
Poco tiempo después, el ejército ruso penetró en territorio georgiano, en el marco del ya extenso conflicto en la región separatista georgiana y pro-rusa Osetia del Sur.
Teniendo como antecedente el mencionado ataque a Estonia, como prueba cierta e irrefutable la complejidad de la operación, y como telón de fondo el problema osetio y la subsiguiente intervención militar; fue fácil para las autoridades georgianas culpar

de lo sucedido a Moscú. Reforzando esta teoría, podemos destacar que incluso fue atacado un medio de comunicación ruso que en sus editoriales sostenía la legitimidad de la posición georgiana sobre Osetia.
No existen pruebas de la participación del gobierno ruso en el suceso, pero los virus que sabotearon las redes georgianas fueron esparcidos desde Rusia. Si, tal como parece, Moscú estuvo tras la operación, habría actuado aquí contra un Estado enemigo –Georgia-, pero también, de manera igualmente ilegítima, contra un medio de comunicación propio. Es decir: la operación constituyó un ataque cibernético a un Estado soberano, y una represión y censura cibernética a una expresión ideológica. Diríamos entonces que fue un acto de agresión internacional y un acto de totalitarismo interno.
Por otro lado, si efectivamente Moscú diseñó los ataques, la guerra de Osetia fue librada sobre la tierra del Cáucaso, pero también – aunque limitándose fundamentalmente a entorpecer la actuación del gobierno georgiano y a hacer propaganda en su contra- en el ciberespacio. Y si bien, pese a la coordinación, los ataques informáticos no lograron ventajas en el campo militar, esto se debió en buena medida a que Georgia no es un Estado que tenga sus defensas tan estrechamente vinculadas a la red, como sí las tienen otros.
A consecuencia de estos hechos, tres países –Estonia, Letonia y Polonia-, se ofrecieron a recibir los sitios web del gobierno georgiano, confiando en que sus sistemas son más difíciles de violar. De manera muy sutil, estamos frente a una alianza en el campo cibernético. No son aquí las fuerzas armadas de un Estado las que ocupan bases militares en otro para protegerlo, sino los servidores de un Estado los que pueden –de manera análoga- defenderlo de agresiones extranjeras.

Los casos mencionados son los que más repercusión han tenido en los medios internacionales. No son sin embargo, ni los primeros ni los últimos.
En septiembre del año 2003, el servicio de inteligencia de Taiwán determinó que hackers que operaban desde la China continental, habían contaminado con virus los sistemas informáticos de al menos cincuenta importantes compañías privadas, y cerca de treinta agencias del gobierno de Taipei. Entre ellas: la policía, el Ministerio de Defensa, el Banco Central y la Junta Electoral. Inmediatamente, -en una decisión poco habitual-, el gobierno de la isla hizo público el ataque y la información referida a los medios de combatir el virus. Paralelamente recomendó no comprar softwares desarrollados en China.
Las relaciones entre la China continental y Taiwán nunca fueron fáciles. Desde que la isla se independizara de facto, al ser el bastión de la resistencia nacionalista contra las fuerzas comunistas de Mao que ganaron la guerra civil; China no ha dejado de reclamar el territorio y considerarlo como una provincia rebelde. En una de las periódicas escaladas de tensión entre los dos gobiernos, transcurrieron los hechos relatados. La implicancia del gobierno chino en ellos, parece poco discutida.

Año 2009: un ciber-ataque tiene como blanco a algunas instituciones públicas y privadas surcoreanas. La inteligencia militar de ese país señaló que el ejército norcoreano posee un laboratorio informático donde sus “piratas” organizaron la destrucción de sus redes informáticas. El rastro del ataque, sin embargo, no logró

conducir a ciencia cierta hasta Pyongyang. Fue seguido por el Reino Unido, Florida y la Argentina; pero luego la pista se perdió en el ciberespacio.

III- INTERNET Y LAS AGRESIONES SEGÚN QUIÉN LAS REALIZA

Los actos delictivos realizados desde la Internet, pueden asimilarse a los realizados en el mundo físico:

Los delitos realizados por individuos particulares, mediante la informática, son análogos –y muchas legislaciones positivas ya han dado cuenta de ello- a los delitos convencionales. Un robo de un banco a mano armada, es similar a una transferencia ilegítima entre cuentas. Un acto vandálico de destrucción de archivos, es equivalente al envío de un virus destructor de datos. Un espionaje tradicional no difiere en su esencia de una infiltración en una red ajena. Un fraude electrónico es totalmente asimilable a uno personal. La pornografía infantil impresa no es más ni menos grave que la digitalizada.

Cuando son grupos a los que podemos denominar "terroristas" –sin desviarnos a la casi imposible definición del término-, los que realizan actos que los identifican como tales, mediante Internet, podemos hablar, no ya de ciber-delitos sino de ciber-terrorismo. El sabotaje físico a la red de comunicaciones de la OTAN en Afganistán, por ejemplo, es equivalente a un sabotaje cibernético de ese sistema. La apología o la financiación del terrorismo que se hace de forma material, no dista de la que se hace mediante Internet.

Cuando desde un Estado se organiza un acto de fuerza interno, fuera del marco de la ley, estamos hablando de violación del Estado de Derecho, o incluso de terrorismo de estado. Estos actos pueden realizarse en buena medida, también desde la red: censuras, difamaciones, represión, amenazas, destrucción de archivos, violación a la intimidad…

Finalmente, cuando un Estado realiza ataques a otro Estado soberano, estamos frente a una agresión internacional. Esta agresión puede tener como blanco el poder militar del otro Estado, pero también su organización civil, e incluso a sus particulares. Análogamente, estos ataques pueden llevarse a cabo también mediante la Internet. Y debe observarse que la agresión a blancos civiles es más grave que la agresión a blancos militares, pues en principio la primera viola las reglas que deben respetarse en los conflictos armados.

Para todos estos actos, la red da una ventaja al agresor: el anonimato. Es más laboriosa la persecución de delitos informáticos, que la persecución de delitos comunes. De allí que se requieran unidades especializadas para aquel fin.

El terrorismo informático también es más difícil de identificar y detener. Y asimismo es más difícil establecer si existe algún Estado que les dé apoyo, cuál es ese Estado. Diciembre de 2009: Un autodenominado "ciber ejército de Irán" bloqueó durante horas una red social que cuestionaba la polémica elección que permitió a Mahmud Ahmadineyad seguir en la presidencia persa. A su vez, difundió por ese medio mensajes en contra de los Estados Unidos. Siempre quedará la duda de hasta qué punto el gobierno de Teherán fue un tercero ajeno a ese hecho.

Durante la última campaña presidencial estadounidense, tanto el candidato Demócrata y posterior vencedor de la contienda –Obama-, como el Republicano –McCaine-, fueron víctimas de espionaje cibernético realizado por hackers, tendiente a hacerse con la información de sus tendencias sobre política internacional. Las miradas del pentágono apuntaron a Pekín, aunque, como siempre, sin pruebas.
En este sentido: la actuación ilegítima interna de un Estado, realizada mediante la red, puede fácilmente camuflarse y adjudicarse la culpa a grupos vandálicos o terroristas. Ese fue el argumento de Rusia en el ya mencionado caso georgiano. Según la versión de Moscú, fueron civiles rusos, ajenos al gobierno, quienes sabotearon el diario que defendía la soberanía de la república caucásica. Y dicha versión no pudo ser probada falsa. A su vez, las agresiones internacionales no pueden ser fácilmente adjudicadas a un Estado, y esos actos pueden –al igual que en el caso anterior- ser imputados a particulares, más o menos organizados. Las supuestas agresiones rusas a Estonia y Georgia, las chinas a Taiwán y las norcoreanas a Corea del Sur; no dejaron tras de sí a un autor probado.
En cualquier caso, frente a una situación dada, no es fácil determinar el agresor y por ende calificar al acto como simple delincuencia, terrorismo, actividad ilegítima interna de un Estado, o agresión internacional.
En 2005, por ejemplo, se efectuaron ataques cruzados entre hackers chilenos y peruanos, que afectaron a instituciones públicas y privadas de ambos países. En enero de 2007, un ataque que se identificó a sí mismo como peruano, dejó inoperante una parte relevante del sistema de información del gobierno de Chile. En 2009, hackers chilenos penetraron en el portal de la Presidencia de Perú, sustituyendo la foto de presidente Alan García, por la del libertador trasandino Bernardo O' Higgins.
En el presente año 2010, los ataque cruzados se han recrudecido. La idea de simple vandalismo puede dejar lugar a la de nacionalismo agresivo organizado, sobrevolada siempre por la sombra de la acusación formal peruana al gobierno de Chile, sobre espionaje, efectuada el año pasado.

En el sentido más estricto del término, sólo podemos decir que hay un ciber-ataque propio de una ciber-guerra, cuando un Estado ataca a otro a través de Internet, ya sea realizado mediante sus organismos tradicionales o de individuos estrechamente vinculados a ellos. En los demás casos, habrá simplemente una agresión cibernética, vandálica. A lo sumo, si la acción es calificable no ya de "vandálica" sino de "terrorista", podrá, eventualmente, ser englobada en el rótulo de "guerra contra el terrorismo". En este caso contra el ciber-terrorismo.
Salvo inoperancia manifiesta por parte de un Estado desde el que se hace un ciber-ataque hacia otro, parece difícil hacer responsable a aquél por la agresión –responsabilidad por omisión-

IV - DISTINTOS TIPOS DE INTERVENCIÓN ILEGÍTIMA EN LA RED

Dentro del conjunto de actos ilícitos que vulneren o atenten contra la soberanía de un Estado, podemos destacar:
Espionaje. Aquí, Internet se utiliza para obtener ilegítimamente información. Esta información puede pertenecer a un particular, o a un organismo público. En principio, en lo que refiere a ciberguerra, sólo es relevante el espionaje a organismos públicos.

Sin embargo, ciertos particulares pueden tener un papel clave en alguna función estatal. V.g.: proveedores de armamentos para el Estado.
Dentro de los organismos públicos, la información puede referir a cuestiones militares o civiles. Ambas son relevantes, pues si bien sólo las primeras permiten obtener una ventaja táctica, las civiles pueden permitir a un Estado ventajas económicas o políticas.
El espionaje cibernético, es totalmente asimilable al espionaje tradicional. Y, en principio, no supone una agresión a otro Estado en los términos del Derecho Internacional. Aunque, obviamente, tanto uno como otro, de ser descubiertos, permiten la persecución de sus actores y dan lugar a tensiones diplomáticas. Basta recordar la mencionada protesta peruana contra el supuesto espionaje chileno en el año 2009.
A medida que se desarrollan servicios de inteligencia con miras a la realización de espionaje informático, los Estados construyen también servicios de contra-inteligencia, para evitar ser espiados. Así pues, la correlación con el espionaje tradicional es completa.
Publicidad indebida. En esta especie de intervención, la Internet se utiliza para hacer apología de una idea. Esta idea, como tal, puede ser legítima o no. Puede oscilar, por ejemplo, desde reivindicaciones hasta calumnias. Pero lo central es que son difundidas en un medio que no les corresponde.
Por ejemplo: en el ya mencionado caso iraní: en un estado democrático, en principio no es incorrecto cuestionar la legitimidad de unas elecciones. Sin embargo, no es correcto cuestionarlas infiltrándose en el portal de una asociación ajena que tiene un pensamiento distinto.
En el también comentado caso entre Chile y Perú: nadie dirá que es incorrecto ensalzar la figura de O` Higgins. Sin embargo, esto no corresponde sea hecho por particulares chilenos en el portal de la Presidencia del Perú.
En la cuestión ruso georgiana: el presidente caucásico sufrió verdaderas calumnias, que tenían el claro objetivo de restarle el apoyo popular en miras al inminente conflicto armado.
O, para buscar un ejemplo contemporáneo, a los potentes parlantes que por años a cada lado del paralelo 38 en la península de Corea, proclamaban al otro bando, respectivamente, las bondades de la democracia del sur y del régimen del norte. Aunque la situación parece equiparable a un bombardeo extranjero, no con explosivos, sino con panfletos; parece por demás forzado entender que hay una agresión. Lo que es evidente, es que, cuando es realizada por un Estado, configura una intromisión indebida en los asuntos internos de otro.
Paralización de sistemas. Aquí, desde Internet se interfieren sistemas informatizados, a fin de entorpecer, confundir o detener los servicios que se presten a través de ellos. Esta operación, también puede afectar a organismos privados o públicos, civiles o militares. Puede interrumpirse, por dar sólo algunos ejemplos: el servicio de pagos por Internet, –organismo privado-, o la extracción de turnos por Internet para trámites jubilatorios –organismo público civil-, o las comunicaciones relativas a una maniobra militar. O, incluso puedo darse la interrupción del servicio de Internet y de telefonía en general.
Como veremos luego, cuando existe una paralización de sistemas, posiblemente podamos hablar ya de agresión. Esta situación es asimilable pues, al sabotaje o a la

ocupación física de las instituciones o instalaciones que prestan los servicios afectados.

En cualquier caso, el efecto de confusión y caos y la sensación de vulnerabilidad que puede ocasionar una paralización masiva de sistemas -aunque sólo sean civiles- puede ser aprovechado para, coordinadamente, el desarrollo de una operación militar. Así ocurrió por ejemplo en Georgia, donde ser vieron afectadas tanto instituciones públicas civiles como militares.

En cuanto a la paralización de sistemas militares, el nivel de indefensión que se puede provocar, es muy alto. La desactivación de las baterías antiaéreas, por ejemplo, dejaría el camino libre a un bombardeo masivo. Otros sistemas de defensa más complejos, podrían ser también totalmente inhabilitados. Piénsese, por ejemplo, en el Escudo Antimisiles de los Estados Unidos.

En muchos casos, la paralización del sistema va acompañada de la ya mencionada publicidad indebida, con la expectativa que ésta sea vista por los usuarios que buscan los servicios del afectado sistema. Durante la Guerra de la Ex Yugoslavia, por dar otro ejemplo además del georgiano, unidades dependientes del ejército serbio lograron penetrar en las computadoras del portaviones norteamericano Nimitz. Y si bien las molestias que provocaron allí fueron menores, aprovecharon la intervención para transmitir imágenes obscenas del presidente Clinton.

Destrucción de sistemas. En este caso, la finalidad de la intervención no es sólo causar una parálisis, sino producir un daño más o menos permanente. Esto ocurre cuando una infiltración mediante Internet permite la destrucción de archivos, registros, programas de trabajo, etc. En el ámbito militar, esta destrucción puede afectar softwares complejos de equipos de defensa computarizados. Y tanto en el militar como en el civil, podría tener además otros efectos de gran trascendencia, tales como la destrucción de satélites.

Esta intervención es análoga a la destrucción física de los mencionados elementos. Indiscutiblemente produce un “daño” -en el sentido jurídico de la expresión-, y no sólo una molestia.

Ataque con armamento ajeno. Esta es la variante más extrema de la ciberguerra. Es la versión más destructiva, pero también la más compleja y por ende la menos probable. Consiste en la infiltración en los sistemas de defensa de un Estado extranjero, no ya para inhabilitarlo o para inutilizarlo de manera perpetua, sino para tomar control sobre él y activarlo sobre el objetivo deseado. Este objetivo puede ser el mismo estado atacado vía Internet –produciéndose así un auto ataque en el mundo físico-, o bien un tercer estado –produciéndose así un ataque en el mundo físico, donde el estado atacante no tiene intención de atacar-.

Los ejemplos de este hipotético ataque pueden ir desde operaciones con consecuencias menores, como la activación de las baterías antiaéreas al paso de los aviones propios; pasando por operaciones con consecuencias graves, como la activación de misiles convencionales sobre el territorio propio; hasta consecuencias catastróficas, como la activación de armamento nuclear.

Indudablemente, no hay diferencia entre este ataque y un ataque convencional.

Incluso en el ámbito civil, determinadas infraestructuras pueden ser utilizadas como armamento. Piénsese por ejemplo en la intervención en la red de control de una presa informatizada, o de una central nuclear. La primera, con la apertura provocada e

indebida de sus compuertas, podría causar inundaciones inconmensurables. La segunda, con un fallo intencional, podría provocar un nuevo Chernobil.
Este escenario que actualmente parece por demás irreal, muy probablemente vaya creciendo en verosimilitud con el transcurso de los años.

V- SITUACIÓN DEL DERECHO EN RELACIÓN A LA CIBERGUERRA

Las intervenciones ilegítimas en la red tienen en la actualidad una tímida regulación jurídica, inferior a la que se considera necesaria para que el Derecho pueda ponerse medianamente a la par de los adelantos tecnológicos, y deje de observarlos, estático, cómo se alejan a la distancia. Algunos Estados, por ejemplo, tienen una regulación aceptable sobre delitos informáticos. Otros, incluso podríamos decir que correcta. Pero los más, siquiera llegan a lo primero.
Lo que refiere a ciberguerra, es aún más complejo. Porque, como ya dijimos, en su sentido más estricto implica necesariamente la participación de al menos dos Estados. Y estos estados son los que deben regular, mediante acuerdos entre sí, cuanto concierne a la guerra cibernética.
Sirva como ejemplo de esta dificultad para la regulación internacional, que en materia de delitos informáticos sólo hay un gran tratado: el Convenio sobre Delitos Cibernéticos del Consejo de Europa –también conocido como "Convenio de Budapest"-, de 2001, ratificado por algunas decenas de países.
Como lo hicieran ya en su momento con la guerra convencional, los Estados deben determinar, en lo que refiere a ciberguerra, entre otras cuestiones: qué se considerará un ataque –cibernético-, y qué tipos de ataques estarán permitidos en los conflictos armados y cuáles no –es decir: el *ius in bellum*-.

VI – PRINCIPIOS GENERALES DE LA COMUNIDAD INTERNACIONAL, APLICABLES A LA CIBERGUERRA

Más allá de las carencias regulativas a las que hicimos y haremos mención, existen una serie de principios legales claros, que rigen en el ámbito de la comunidad internacional, y que deben ser entendidos como marco regulatorio vigente al momento de analizar la ciberguerra. Decimos que son principios internacionales, porque constan en documentos aceptados de manera casi unánime por los diferentes Estados –Carta de las Naciones Unidas, Protocolos Adicionales a los Convenios de Ginebra-; o bien en otros que, si bien son circunscriptos, se entienden como perfectamente válidos y paradigmáticos .
Por un lado: estos principios pueden orientar –y de hecho orientan- la solución a las interrogantes que no tienen una respuesta específica. Y por otro: son el parámetro sobre el cual, a futuro, corresponde implementar una regulación puntual a nivel internacional.
Como principios, podemos destacar los siguientes:
- **Prohibición del uso de la fuerza**. Es decir: los Estados no deben resolver sus diferencias por medios armados. La Carta de las Naciones Unidas indica como principio: "*Los Miembros de la Organización arreglarán sus controversias internacionales por medios pacificos de tal manera que no se pongan en peligro ni la paz y la seguridad internacionales ni la justicia. Los Miembros de la Organización,*

en sus relaciones internacionales, se abstendrán de recurrir a la amenaza o al uso de la fuerza contra la integridad territorial o la independencia política de cualquier Estado, o en cualquier otra forma incompatible con los Propósitos de las Naciones Unidas." (art. 2.3 y 2.4) Esto se corresponde con los objetivos de la Organización, marcados por la misma Carta (Art. 1.1 y concordantes)

El Tratado de la OTAN establece: "*Las partes se comprometen a (…) a abstenerse en sus relaciones internacionales de recurrir a la amenaza o al empleo de la fuerza de cualquier forma que resulte incompatible con los propósitos de las Naciones Unidas." (art. 1) La Carta de la OEA, determina que: "Los Estados americanos reafirman los siguientes principios: (…) g) Los Estados americanos condenan la guerra de agresión: la victoria no da derechos. (…) i) Las controversias de carácter internacional que surjan entre dos o más Estados americanos deben ser resueltas por medio de procedimientos pacíficos. (…) (art. 3)" "El territorio de un Estado es inviolable; no puede ser objeto de ocupación militar ni de otras medidas de fuerza tomadas por otro Estado, directa o indirectamente, cualquiera que fuere el motivo, aun de manera temporal. No se reconocerán las adquisiciones territoriales o las ventajas especiales que se obtengan por la fuerza o por cualquier otro medio de coacción."* (art. 21) "*Los Estados americanos se obligan en sus relaciones internacionales a no recurrir al uso de la fuerza, salvo el caso de legítima defensa, de conformidad con los tratados vigentes o en cumplimiento de dichos tratados."* (art. 22)

- **Derecho a la legítima defensa, individual y colectiva**. Es decir: si un Estado es atacado, puede defenderse, y puede solicitar la ayuda de otros Estados. La Carta de las Naciones Unidas especifica que: "*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. (…)"* (Art. 51)

El Tratado de la OTAN establece: "*Las Partes acuerdan que un ataque armado contra una o más de ellas, (…) 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, ayudar a la Parte o Partes atacadas, adoptando (…) las medidas que juzgue necesarias, incluso el empleo de la fuerza armada, para restablecer la seguridad* (…)" (art. 5) La Carta de la OEA, determina: "*Los Estados americanos reafirman los siguientes principios: (…) h) La agresión a un Estado americano constituye una agresión a todos los demás Estados americanos. (…)* (art. 3. Repite en art. 28)" "*Si la inviolabilidad o la integridad del territorio o la soberanía o la independencia política de cualquier Estado americano fueren afectadas por un ataque armado o por una agresión que no sea ataque armado, (…) o por cualquier otro hecho o situación que pueda poner en peligro la paz de América, los Estados americanos en desarrollo de (…) la legítima defensa colectiva, aplicarán las medidas y procedimientos establecidos en los tratados especiales, existentes en la materia.*" (art. 29)

- **No intervención**. Es decir: No corresponde a un Estado, intervenir en los asuntos de otro. No sólo un Estado no debe agredir a otro, sino que no debe entrometerse en sus asuntos internos. La Carta de las Naciones Unidas indica que: "*Ninguna*

disposición de esta Carta autorizará a las Naciones Unidas a intervenir en los asuntos que son esencialmente de la jurisdicción interna de los Estados, (…)" (Art. 2.7) La Carta de la OEA, por su parte establece que: *"Los Estados americanos reafirman los siguientes principios: b) El orden internacional está esencialmente constituido por el respeto a la personalidad, soberanía e independencia de los Estados"* (art. 3) *"Ningún Estado o grupo de Estados tiene derecho de intervenir, directa o indirectamente, y sea cual fuere el motivo, en los asuntos internos o externos de cualquier otro. El principio anterior excluye no solamente la fuerza armada, sino también cualquier otra forma de injerencia(…)"* (Art. 19)

- Los civiles no pueden ser atacados en los conflictos armados. Este es un principio básico del Derecho Humanitario que corresponde resaltar aquí. El Protocolo I Adicional a los Convenios de Ginebra manda que: *"A fin de garantizar el respeto y la protección de la población civil y de los bienes de carácter civil, las Partes en conflicto harán distinción en todo momento entre población civil y combatientes, y entre bienes de carácter civil y objetivos militares y, en consecuencia, dirigirán sus operaciones únicamente contra objetivos militares."* (art. 48) Es persona civil, cualquiera que no sea militar (Conf. art. 50) *"Se entiende por "ataques" los actos de violencia contra el adversario, sean ofensivos o defensivos."* (Art. 49.1) *"(…) se observarán en todas las circunstancias las normas siguientes. No serán objeto de ataque la población civil como tal ni las personas civiles. Quedan prohibidos los actos o amenazas de violencia cuya finalidad principal sea aterrorizar a la población civil. (…) Se prohíben los ataques indiscriminados. Son ataques indiscriminados: a) los que no están dirigidos contra un objetivo militar concreto; b) los que emplean métodos o medios de combate que no pueden dirigirse contra un objetivo militar concreto; o c) los que emplean métodos o medios de combate cuyos efectos no sea posible limitar conforme a lo exigido por el presente Protocolo; y que, en consecuencia, en cualquiera de tales casos, pueden alcanzar indistintamente a objetivos militares y a personas civiles o a bienes de carácter civil.(…)"* (Art. 51.1, 51.2, y 51.4) *"Los bienes de carácter civil no serán objeto de ataque ni de represalias. Son bienes de carácter civil todos los bienes que no son objetivos militares en el sentido del párrafo 2: Los ataques se limitarán estrictamente a los objetivos militares. En lo que respecta a los bienes, los objetivos militares se limitan a aquellos objetos que por su naturaleza, ubicación, finalidad o utilización contribuyan eficazmente a la acción militar o cuya destrucción total o parcial, captura o neutralización ofrezca en las circunstancias del caso una ventaja militar definida*" (Art. 52.1 y 52.2)

VII – INTERROGANTES LEGALES A RESOLVER

Entre las cuestiones que deja sin solución el vacío legal vigente, podemos destacar las siguientes:

- ¿Qué actos -de los antes mencionados-, se consideran una agresión? Como ya dijimos, muy posiblemente no el espionaje. En relación a la publicidad ilegítima, las controversias serán mayores. Como ya vimos, indudablemente es una intervención ilegítima en los asuntos internos de otro Estado, y puede incluso llegar a interpretarse como una promoción de la violencia contra el orden instituido.

La paralización de sistemas, por su parte, también puede prestarse a interpretaciones dispares. Posiblemente deba evaluarse la relevancia del sistema atacado, la modalidad, la duración del ataque, y su objetivo mediato.
En cuanto a la destrucción de sistemas y el ataque con armamento ajeno, difícil es no entender que estamos frente a una agresión de otro Estado.
-¿Frente a un ataque cibernético, el Estado atacado debe limitarse a defenderse y a contraatacar por los mismos medios, o está autorizado en razón a su derecho de legítima defensa a responder con todos los medios que tenga a su alcance?
La primera solución puede parecer desproporcionada en el caso de paralización de sistemas e incluso en el de destrucción de sistemas, pues la ciberguerra tiene una característica que luego analizaremos: en la mayoría de sus variantes, no causa víctimas humanas. Sin embargo, la segunda opción parece ridícula. Obligaría, por ejemplo, a un Estado militarmente avanzado pero tecnológicamente atrasado, a verse vapuleado en el ciberespacio, sin poder responder. Y obligaría también a limitar la acción al campo cibernético escogido por el enemigo, y resignar las ventajas que pudiera presentarle el mundo físico.
En este sentido, muchos Gobiernos han dejado claro que un ataque cibernético sería respondido con todos los medios a su disposición. Esto es, la guerra convencional.
-Si un Estado considera estar siendo atacado cibernéticamente por otro: ¿Puede pedir ayuda a terceros Estados, alegando el derecho de defensa colectivo? ¿Puede solicitar la ayuda de otros Estados en el marco de convenios de defensa, tales como la OTAN? Todo parece indicar que sí, pero nada se ha escrito al respecto. Y este vacío deja margen –aunque estrecho- para que algún Gobierno se niegue a intervenir en un conflicto, cuando un pacto de defensa lo ha obligado a ello.
-¿Qué tipo de ataques están permitidos? Siendo que, incluso en la guerra, no todos los medios y no todas las acciones están permitidas: ¿Los ataques cibernéticos constituyen un medio prohibido de hacer la guerra? En principio, parecería que no. Más aún: como en general los ataques cibernéticos no causan bajas humanas –salvo casos extremos-, pueden aparentar ser el modo más civilizado y menos destructivo de guerrear. Sin embargo, surge otra problemática: ¿Qué está permitido atacar cibernéticamente?
En principio, según el *ius in bellum*, sólo pueden ser blanco de ataques las fuerzas combatientes del Estado enemigo. De allí que, parecería que la ciberguerra sólo debería poder afectar a instituciones o instalaciones militares. Se entendería que no es correcto entonces el ataque a instituciones gubernamentales civiles, ni a otros centros meramente administrativos, ni a entidades particulares como bancos, grandes empresas, etc. Pues sólo tendrían como objeto causar molestias y terror en la población no combatiente, y esto está prohibido por el Derecho Internacional.
Sin embargo, en contra de esto también podría llegar a alegarse que los mencionados ataques, como ya dijimos, no causan bajas humanas, y por lo tanto son incluso más humanitarios que los ataques armados contra fuerzas combatientes. Por nuestra parte, descartamos esta última postura, alegando que este vacío legal debe ser completado con los principios generales del Derecho de Guerra y el Derecho Humanitario.

Todos estos vacíos legales, pueden hacer que los Estados tengan menos reparos en realizar intervenciones ilegítimas cibernéticas, que intervenciones ilegítimas en el mundo físico. Esto motivado en las dudas sobre si el acto que realizan puede ser

calificado de agresión, sobre los medios con los que puede responder el Estado agredido y sobre la intervención que harán terceros Estados alineados con él; sumada a la ya referida tarea hercúlea de probar la autoría el hecho.
Por otro lado, los vacíos legales hacen que en la práctica cualquier objetivo sea susceptible de ser agredido, pretendiendo el agresor imputado el beneficio de la duda y alegando la falta de derramamiento de sangre.
El anonimato en la agresión, a su vez, se ve fortalecido por la inexistencia de obligaciones universales en lo que hace a cooperación en materia de ataques cibernéticos. Desviando las acciones a través de Estados con el cual el Estado agredido no tiene buenas relaciones diplomáticas, el agresor se asegura que será aún más complejo seguir su rastro, pues el Estado utilizado como puente no estará obligado a brindar la información necesaria para permitir la prosecución del rastreo.
Basta pensar en el mencionado caso surcoreano. Si el seguimiento de la pista del ataque fue complejo pese a la buena disposición de los países involucrados –el Reino Unido, Estados Unidos, etc.-; cuán más dificultoso es el caso en donde éstos ponen trabas burocráticas al pedido de información.

VIII – LOS CARACTERES DE LA CIBERGUERRA

De todo lo antes dicho, podemos sintetizar que la ciberguerra se caracteriza por ser:
-De difícil detección del agresor. La ciberguerra, como ya vimos y ejemplificamos, se destaca por lo dificultoso que resulta la determinación del autor del ataque. En muchos actos es difícil identificar si se trata de un vándalo particular, de una organización terrorista, de un Estado extranjero, o de alguno de los dos primeros con el visto bueno de este último. Y, en todos los casos, resulta más complejo aún el indicar qué sujeto en particular fue el agresor.
-No regulada expresamente por el Derecho Internacional. Como ya analizamos también, el Derecho Internacional nada dice expresamente en relación a la ciberguerra. Sólo pueden considerarse referentes a ella, algunos principios básicos de este Derecho ya citados, a los que podemos agregar otros principios del *Ius in bellum* –además del que manda la no agresión a civiles-. Quedan por responder las interrogantes antes mencionadas: ¿Qué ataques cibernéticos son una agresión? ¿Qué respuesta se puede dar ante ellos? ¿Qué tipo de ataques están permitidos y cuales prohibidos…? Mientras esto no se responda, no habrá certeza sobre qué se considera un acto de guerra, y qué actos pueden realizarse dentro de una guerra.
En la práctica, los Estados han llenado en parte estos vacíos. Como ya dijimos: declarando que un ataque cibernético será considerado como un ataque convencional –la dificultad es probar la autoría-, y no discriminando blancos civiles y militares.
Como ya vimos, la falta de regulación internacional en lo que hace a cooperación, contribuye a acentuar el carácter de difícil detección del agresor. Pues los Estados bien pueden no colaborar con rastreo de las acciones en la red que utilizaron su espacio para agredir a terceros.
-Susceptible de dañar con más fuerza a los países más informatizados. Este tipo particular de guerra, hace que los Estados que en principio están más preparados para afrontar los conflictos armados, por tener mayor tecnología militar y equipos más avanzados, y estén más informatizados también en el aspecto civil; sean los que más perjuicios pueden sufrir. Quienes, por el contrario, dependen menos de la informática, presentan un blanco menor, y de ser afectados, las consecuencias para ellos serán de

menor relevancia. Al mencionar el caso georgiano, por ejemplo, hicimos referencia, a la poca incidencia del ciber-ataque supuestamente ruso sobre el país, por no estar este país altamente informatizado.

-En principio, no sangrienta. Como ya comentamos también, en general, la ciberguerra no implica pérdida de vidas humanas. Tanto la paralización de sistemas, como su destrucción permanente, no traen aparejadas –en principio-, muerte alguna ni grandes destrucciones materiales. En este sentido, efectivamente, la ciberguerra tiene un marcado carácter humanitario.

Sin embargo, es ilusorio entender que marcará el final de los conflictos sangrientos. No es realista creer que las guerras del futuro se librarán sólo desde ordenadores, y que cuando un Estado se vea superado, y paralizado su poderío militar o su organización civil, se rendirá. Pues sería muy dificultoso llegar a tal extremo, y en todos los casos habrá fuerzas convencionales que escapen a la amenaza cibernética y procuren la guerra tradicional.

Más allá de esto, se debe destacar que no por ser no sangrienta, la ciberguerra puede tener cualquier blanco en sus ataques. El Derecho Internacional retrocedería si se permitiera que instituciones civiles o particulares pudieran ser afectadas vía Internet. Dado el nivel de desarrollo tecnológico de la actualidad, cualquier afección a sistemas civiles ocasionaría a los no combatientes trastornos tan grandes, que no pueden ser aceptados por el Derecho. Como ya dijimos, el vacío legal sobre los objetivos de la ciberguerra, entendemos debe completarse con los principios generales del Derecho de Guerra y el Derecho Humanitario. Caso contrario, la guerra cibernética, si bien no sería sangrienta, sería por demás destructiva para toda la sociedad.

Por otro lado, no debemos perder de vista, que la ciberguerra puede en un futuro no muy lejano llegar a tener su variante más peligrosa: el secuestro de armamento. Y, en ese caso, su carácter de "no sangrienta" dejará de existir.

-Económicamente no muy onerosa. En relación a los costos que actualmente tiene la adquisición y el mantenimiento de las armas tradicionales para hacer la guerra –ejército, armada, fuerza aérea- con su respectivo personal y equipamiento: tanques, submarinos, aviones de combate, misiles,….; la guerra cibernética resulta ser poco onerosa. Basta con tener una serie de ordenadores avanzados y personal capacitado, para poder dañar a la distancia al enemigo. En cuanto a la capacitación del personal, incluso puede que ésta ya se haya producido de manera natural en la vida de los individuos, si el reclutamiento centra sus esfuerzos en quienes tienen experiencia como hackers.

Claro está, que la destrucción de un ciberataque no es comparable a la fuerza destructiva de un misil o una bomba. Pues, como ya dijimos, la ciberguerra en principio no produce el derramamiento de sangre, ni tampoco grandes destrucciones materiales. Pero cumple igualmente con la idea de afectar al enemigo. Máxime si, como se ha hecho hasta ahora, no se distinguen blancos civiles de militares.

En consecuencia, la guerra cibernética se ubica junto a la guerra química y la guerra bacteriológica, en el grupo de las denominadas "armas de los pobres". Y, como ya se vio, como contrapartida, puede dañar más los países informatizados, que, *a grosso modo*, son los países desarrollados o los países ricos.

El carácter de "económicamente no onerosa", hará que la guerra cibernética, de a poco, sea adoptada por los Estados pobres. En su momento, como ya vimos, fue

utilizada incipientemente por la Ex Yugoslavia. Y, como ya está ocurriendo, también darán uso de ella los grupos terroristas.

IX- PERSPECTIVAS Y CONCLUSIONES

En este trabajo, hemos tratado de definir a grandes rasgos, ejemplificar, describir y caracterizar la ciber guerra. Sólo basta decir, que esta nueva forma ingeniada por el ser humano para atacar a sus semejantes, irá creciendo en su utilización e intensidad, hasta ser un elemento relevante en los conflictos armados de este siglo. Incluso, puede que ya haya avanzado más de lo que advertimos.

Ante la Asamblea General de Naciones Unidas, el presidente estonio Hendik Ilves –luego del ciberataque a su país- declaró que la amenaza que representa la ciberguerra es subestimada por el mundo. Y que un número grande de ataques son mantenidos en secreto por razones de seguridad para los mismos Estados que los han sufrido.

El mundo se está preparando pues, para este nuevo tipo de conflicto.

Para dar un ejemplo: la OTAN ha establecido el **"**Centro Cooperativo de Ciberdefensa de Excelencia**" –**conocido más comúnmente como "K5"-, en las afuera de Tallin, Estonia. Allí, se hacen simulacros y planificaciones sobre cómo la Organización respondería a ataques cibernéticos.

A su vez, comienza a visualizarse lo que podrá eventualmente ser una carrera armamentística en el ciberespacio. Grandes potencias toman esta cuestión muy en serio, y proceden a aprontarse para obtener buena posición en este nuevo campo bélico. Estados Unidos, China, Rusia, el Reino Unido, Israel,…. son los nombres que suenan para asumir la primacía en este espacio. Y otros tantos, no quieren quedar rezagados e indefensos: Alemania, Francia, España…

Pero más allá de la preparación técnica, el mundo necesita una preparación jurídica, en lo que hace a acuerdos de cooperación y de regulación. La cooperación internacional es imprescindible ante la ciberguerra, fundamentalmente por el mencionado carácter de difícil detección del agresor. Los Estados deben comprometerse a dar la información y asistencia necesarias para el rastreo de ataques, cualquiera sea su procedencia y cualquier Estado o particular esté detrás de ellos.

La regulación internacional, por otro lado, es menester para suplir los vacíos legales mencionados anteriormente. Entre más se detalle qué está permitido hacer y que no en materia de ciberguerra, siempre que la solución sea congruente con los principios internacionales humanitarios y el Derecho en la guerra; menos sufrimiento traerá su acontecer. Al menos, en cuanto se trate de una guerra abiertamente declarada. La ciberguerra obliga a los Estados a reconocerse como parte de una gran comunidad internacional, de la que no pueden desentenderse; que así como los beneficia, también los afecta y los amenaza.

Como ya dijimos, el papel de la ciberguerra en los conflictos bélicos del futuro, irá siendo mayor. Posiblemente no llegue a ser la *prima donna* de la guerra, pero es un arma que cobrará más protagonismo. Y este hecho no debe llamarnos la atención.

En la enumeración de elementos que se volcaron a la guerra o nacieron para ella que hicimos al inicio de este trabajo, hubo una omisión voluntaria. No hablamos del origen de Internet. La red que hoy todos conocemos, tuvo sus fundamentos en la llamada ARPANET: red de comunicación del ARPA –siglas en inglés de la Agencia de Proyectos de Investigación Avanzada; dependiente del Departamento de Defensa

de los Estados Unidos-; actualmente llamada DARPA. Durante la Guerra Fría, se ideó la conexión de los ordenadores militares, para posibilitar el manejo de los sistemas y la tenencia de la información imprescindible desde cualquier punto del país; ante el riesgo de un ataque nuclear soviético. Sólo después la red se utilizó para fines académicos, gubernamentales civiles, y privados.
Así pues: no corresponde decir que Internet se haya volcado al un fin bélico, sino más bien que la red se ha reencontrado con fin militar para el que fue ideada originalmente, y que quedó opacado cuando el mundo advirtió su valor en otras áreas.

En conclusión: a las armas ya terribles del furibundo Marte se les ha reincorporado una que él tenía casi olvidada. Y esta arma atípica lleva implícita las aladas sandalias de Mercurio, que hacen al atacante capaz de cruzar en segundos los distintos continentes; y el yelmo de Plutón, que le vuelve invisible. Y le es sencillo hacer uso de esta arma, pues el costo que implica es escaso.
Esta arma puede en principio no derramar sangre, pero como la égida adornada con la cabeza de Medusa, puede paralizar ciudades enteras y causar el pánico. Y utilizada de su modo más terrible, es capaz de producir una destrucción y muerte inusitadas.
El mundo puede, en razón de este hecho, lamentar la idiosincrasia humana, capaz de volver agresivo aquello que tanto le ha servido para el progreso. El mundo debe –sin alarmarse- prepararse, logística y jurídicamente, para afrontar la amenaza que lentamente se acrecienta. Y esa preparación requerirá esfuerzos conjuntos de los Estados. *La comunidad internacional debe verse a sí misma como tal, y actuar en consecuencia.*
…Lo que no puede hacer jamás el mundo, es sorprenderse.

FUENTES MENCIONADAS Y FUENTES DE INTERÉS

Fuentes jurídicas mencionadas:

Convenio sobre Delitos Cibernéticos del Consejo de Europa ("Convenio de Budapest"), de 2001 - Carta de las Naciones Unidas - Carta de la Organización de Estados Americanos - Tratado de la O.T.A.N. - Protocolo I Adicional a los Convenios de Ginebra

Bibliografía jurídica:

BARBOZA, Julio, *Derecho Internacional Público*, Zavalía, Bs. As., 2004
DIEZ DE VELASCO, Manuel, *Instituciones del Derecho Internacional Público*, Tecno, Madrid, 2007
KALSHOVEN Frits y ZEGVELD Liesbeth, *Restricciones en la conducción de la Guerra*, Comité Internacional de la Cruz Roja, Ginebra, 2001

Bibliografía jurídica on line:

MOLINA, José María. *La defensa del Estado en la Sociedad de la Información: Una perspectiva Iberoamericana.*
http://www.alfa-redi.org/rdi-articulo.shtml?x=1247
MOLIST, Mercedes. *Juegos de infoguerra.*
http://www.alfa-redi.org/rdi-articulo.shtml?x=319

Fuentes informativas de interés a consultar, buscando por "ciberguerra":

http://www.lanacion.com.ar - http://www.clarin.com/diario
http://www.elmundo.es - http://www.elpais.com
http://www.maestrosdelweb.com